

Hacked Silence:

Journalists and Surveillance – Addressing legal and regulatory challenges

Research conducted by

Paula Ligia Martins

Commissioned by

International Federation of Journalists (IFJ)

Disclaimer: This publication was co-funded by the European Union.

Its contents are the sole responsibility of the International Federation of Journalists and do not necessarily reflect the views of the European Union.

September 2026

This report has been published as part of the [Brave Media project](#) – a global programme supporting independent media and public interest journalism.

Public interest media play a vital role in democracy and development – yet in 2025, press freedom reached a historic low, with conditions for journalism now rated “difficult” or worse in more than half the world’s countries, amid intensifying political, legal and economic pressure. Across countries, journalists face political and security threats, financial strain, rising mis- and disinformation, and a deepening crisis of trust – which together pose an existential threat to independent media and to democracy itself.

[Brave Media](#) responds to these by supporting locally-led solutions that help media outlets and networks operate safely, build resilience, and continue delivering trusted information to communities in the face of growing political, financial and digital threats.

The project – co-funded by the European Union – is led by [BBC Media Action](#), working in a consortium with eight other organisations: [Arab Reporters for Investigative Journalism \(ARIJ\)](#), [Equal Rights and Independent Media \(ERIM\)](#), [the International Federation of Journalists \(IFJ\)](#), [Fondation Hirondelle](#), [the Media Institute of Southern Africa \(MISA\)](#), [the Samir Kassir Foundation](#), [SembraMedia](#), and the [World Association of News Publishers \(WAN-IFRA\)](#).

Executive summary

As we prepared to launch this report, Greek journalist Thanasis Koukakis's lawyers [announced](#) that they had filed an application with the European Court of Human Rights (ECHR) against Greece over how the national judicial authorities had handled the investigation into the surveillance and spying on the reporter by the Greek National Intelligence Service. Koukakis's phone had been [infected](#) with Predator spyware.

Within days media [reports](#) exposed the largest documented wave of surveillance in Serbia, including the use of the Pegasus spyware.

Surveillance - particularly when carried out by state or large corporate actors - can severely undermine the ability of journalists to do their work. When reporters, editors, or sources are surveilled, the mere knowledge of this practice can chill free expression, discourage investigative reporting, and erode the watchdog role of the press, which is essential to healthy democracies. The effects go beyond the impacts on targets, affecting society as a whole.

But surveillance is, above all, directly related to the safety of journalists. Beyond breaching privacy rights, it can precede or facilitate threats, arbitrary arrests, disappearances, or killings of journalists. It also compromises confidentiality between journalists and their sources, especially whistleblowers, human rights defenders, and victims of abuse. This breach can deter individuals from coming forward with critical information, which limits public access to truth and stifles transparency.

This study was commissioned by the International Federation of Journalists as the second of two studies analysing the tools, methods, impacts and the environment – especially the legal and regulatory environment – in which media operate and developing recommendations which will form the basis of advocacy and lobbying efforts by journalists' unions, associations, media organisations and civil society organisations committed to media freedom and freedom of expression.

The first study [*Global Surveillance of Journalists: A Technical Mapping of Tools, Tactics, and Threats*](#) – published in April 2026 – is an investigative study on the technologies and methodologies used to monitor, target, and intimidate members of the press worldwide. It exposed how journalists across the globe are subject to a systemic infrastructure of control through increasingly sophisticated digital surveillance technologies.

Drawing on interviews with cybersecurity experts, forensic analysts and journalists from diverse parts of the world, as well as technical documentation and verified investigations between 2021 and 2025, it paints a detailed picture of how the act of reporting has become intertwined with the risk of being watched, tracked or hacked.

This second study focuses on the legal and regulatory environment in which journalists and media operate. It draws on a study of the laws, regulatory rules, resolutions, significant legal cases and rulings, adopted by major inter-governmental organisations – the United Nations, European Union, African Union and Organisation of American States.

The scope is global, with further in-depth research drawing on the same 10 primary countries covered in the previous study — India, Pakistan, Kenya, Italy, Serbia, Brazil, Mexico, El Salvador, Lebanon and Jordan.

Across the case studies examined a similar pattern emerges: the convergence of commercial spyware, state intelligence, and weak oversight – a lack of transparency, judicial oversight, legislative or parliamentary accountability and/or independent bodies with the power to investigate and audit.

Even where inter-governmental organisations, individual governments, regulatory or legal authorities have adopted laws or regulations or made rulings which seek to protect media freedom there is a lack of enforcement and processes designed to enhance accountability and transparency are failing.

The case studies help expose the failings and gaps in current legal and regulatory protections for media freedom. The report focuses on six key dimensions: (1) judicial safeguards and due process (e.g. warrant requirements and judicial oversight), (2) legal limits on surveillance (necessity, proportionality, and targeted vs. mass surveillance), (3) oversight and accountability mechanisms (independent regulators, legislative controls), (4) remedies and redress available to individuals, (5) distinctions between general surveillance frameworks vs. spyware-specific rules, and (6) broader regional or systemic patterns.

The analysis reveals emerging patterns, notable contrasts, and persistent regulatory gaps across these diverse jurisdictions, drawing on constitutional norms, statutory laws, and recent case developments.

Across regions and regime types, digital surveillance has shifted from an exceptional, security-led practice to a more normalized, widely available capability, driven by a booming mercenary-spyware market and data-extraction business models. Journalists and their sources now operate in an environment where targeted intrusions and data-driven monitoring are routinely leveraged to chill speech, compromise investigations, and endanger lives.

Legally, there is convergence at the level of principles - legality, necessity, proportionality, independent oversight, and effective remedy - rejecting indiscriminate regimes while permitting targeted, threat-led, reviewable surveillance. But there is persistent divergence in practice, characterised by intelligence and “national security” carve-outs, opaque procurement, weak parliamentary/judicial controls, and near-total regulatory lag around state malware and advanced tooling.

At the country level, the same patterns recur:

- Rules exist on paper, but emergency measures and broad mandates erode safeguards
- Intelligence bodies operate with minimal transparency
- Spyware and exploit procurement outpace law
- Accountability for abuses is rare

The ecosystem is structurally tilted towards opacity and impunity. Rebalancing requires multilayered reforms, including hard law, hard oversight, market discipline and operational resilience for newsrooms and civil society.

This research concludes that journalists around the world are being spied on at an unprecedented scale, and each silent hack or intercepted data strikes at the heart of democracy. Surveillance of the press is a serious threat to journalists’ safety worldwide. When reporters suspect that every call, message, or movement may be watched, they are more likely to avoid sensitive investigations, drop sources, or resort to self-censorship. This is the outcome repressive actors want – a silenced press and a public kept in the dark.

This report is part of a global response – a call to action – to break that silence.

Researcher/Author

Paula Ligia Martins

Paula is a human rights lawyer and global policy expert with more than 20 years of experience working at the intersection of digital rights, media freedom, and international human rights law. Specialized in the analysis of digital policies and practices, including surveillance, freedom of expression, and legal standards affecting journalists and civil society in the Global South.

Methodology:

This study adopts a qualitative, multi-method research design combining in-depth case study analysis and extensive desk research. The goal was to document the legal and regulatory environment governing digital surveillance in which journalists and media operate. It draws on a study of the laws, regulatory rules, resolutions, significant legal cases and rulings adopted by major inter-governmental organisations – the United Nations, European Union, African Union and Organisation of American States.

While the scope is global, this report draws on 10 primary countries – India, Pakistan, Kenya, Italy, Serbia, Brazil, Mexico, El Salvador, Lebanon and Jordan. It draws on detailed studies of the legal norms, cases and practice of selected countries. These case studies have been chosen to illustrate a spectrum of contexts, from democratic states experimenting with ‘lawful interception’ to authoritarian regimes using imported spyware to suppress dissent and control the press. They enable the report to consider the steps necessary to address threats to media freedom posed by surveillance of journalists in a range of diverse situations.

A wider global context – including a focus on the systemic and widespread surveillance carried out by Israel against Palestinian journalists and the impact of surveillance by Russia/Belarus – was covered in our [earlier report](#) which focused on the tools and methods of surveillance. As a result, to avoid duplication, these examples are absent from this report.

The research approach integrated complementary strands – an in-depth analysis of documented surveillance incidents and extensive secondary research using legal, technical and NGO data sources.

This ensured both qualitative depth and empirical verification. The study focused primarily on the legal and regulatory frameworks governing surveillance rather than the technical means, highlighting crucial gaps and failings in protecting media from unlawful surveillance.

More than 90 external sources were reviewed to contextualise the findings. Key references included:

- United Nations, European Union, Inter-American Commission on Human Rights and African Union databases and document libraries
- Amnesty International Security Lab, Citizen Lab, Electronic Frontier Foundation and NGO reports on surveillance of journalists
- NGO and media reports and publications on media freedom and digital repression
- Records of court cases

This combination of sources provided both empirical validation and geopolitical framing for understanding the evolving surveillance ecosystem.

The research was conducted between July and October 2025. It directly informed the:

- global overview of laws and regulations governing surveillance of journalists
- country and regional case studies
- recommendations for IFJ to develop a policy paper for journalists, media institutions and policymakers

In addition to the research study, a number of recommendations have been developed by the IFJ which will be included following this report.

Chapter 1. Setting the scene

In an era defined by ubiquitous connectivity and unprecedented data collection, journalism faces a profound and growing threat: digital surveillance. Once considered a tool for national security and intelligence gathering, surveillance has evolved into a powerful mechanism of control, used not only by authoritarian regimes, but increasingly by democratic states and private actors to monitor, intimidate, and silence journalists. From mass surveillance programs exposed by the Snowden revelations to the proliferation of commercial spyware like Pegasus and Paragon, journalists today operate in an environment where their communications, sources, and movements can be tracked without their knowledge or consent. This report examines how the expansion of surveillance - both mass and targeted - undermines press freedom, disrupts investigative reporting, and erodes the trust and safety essential to democratic accountability. By mapping new technologies, actors, and legal gaps, it highlights the urgent need for stronger protections, regulatory oversight, and global solidarity to defend journalism in the digital age.

This report is divided into two parts. Part I provides an overview of the impact of surveillance on journalism, different types of surveillance in use today, and presents a summary of country case studies – both concerning deployment of digital surveillance and legal frameworks, to finally provide an overview of responding international standards that have emerged. Part II provides a more detailed account of the country case studies, which serve as the basis for the summaries presented in Part I.

1.1 How surveillance threatens journalism

Surveillance - particularly when carried out by state or large corporate actors - can severely undermine the ability of journalists to do their work. When reporters, editors, or sources are surveilled, the mere knowledge of this practice can chill free expression, discourage investigative reporting, and erode the watchdog role of the press, which is essential to healthy democracies. The effects go beyond the impacts on targets, affecting society as a whole.

But surveillance is, above all, directly related to the safety of journalists. Beyond breaching privacy rights, it can precede or facilitate threats, arbitrary arrests, disappearances, or killings of journalists. It also compromises confidentiality between journalists and their sources, especially whistleblowers, human rights defenders, and victims of abuse. This breach can deter individuals from coming forward with critical information, which limits public access to truth and stifles transparency.

Surveillance, however, does not affect all journalists equally. [Research](#) shows that women journalists, LGBTQ+ media workers, and those from marginalized racial or ethnic groups often face amplified harms, and have been frequently subject to harassment, doxxing, and stigmatization. Investigating these dynamics is key to building intersectional protections.

With the rise in the use of digital technologies developed for surveillance purposes, including AI-powered surveillance, Pegasus-style spyware, and data-driven profiling, the landscape of threats to journalism is rapidly evolving. Ongoing research will be needed to understand how constantly evolving technologies are deployed, their human rights implications, and how they can be regulated to prevent misuse.

Mapping such risks helps international organizations, media outlets, and civil society groups to design protective protocols, emergency responses, and advocacy campaigns tailored to specific contexts.

It also allows researchers and advocates to document patterns of abuse, identify responsible actors, and demand accountability. This is particularly important in contexts where surveillance is broadly used to target dissent, manipulate narratives, or obstruct reporting on corruption, human rights violations or state violence.

Research informs evidence-based advocacy, supporting calls for stronger privacy protections, surveillance oversight, whistleblower laws, and digital security measures. It can also help shape regional and international legal frameworks, including those under the UN and regional human rights system and digital governance frameworks.

This is the goal of this study - to provide evidence concerning the critical impact of digital surveillance on journalism. The ultimate objective is to increase journalists' safety and to safeguard and protect democratic values, human rights, and public accountability.

1.2 What do we mean by digital surveillance?

Surveillance is a broad concept involving monitoring behaviour, activities, or information for the purpose of gathering intelligence, influencing outcomes, detecting actions, or managing operations. It includes both physical observation (e.g. CCTV) and the interception of communications or data.

When deployed with the use of, or facilitated by, digital technologies, surveillance can take various forms and degrees of intrusion, ranging from the documentation and monitoring of online activities and communications to the large-scale or targeted collection of digital information.

Targeted surveillance refers to the monitoring of specific individuals, groups, or devices, while **mass surveillance** refers to the indiscriminate or large-scale collection of data across populations, without individualized suspicion.

[Targeted surveillance](#) typically occurs, when legal, within the context of criminal investigations or other legal proceedings and involves tracking the communications of a specific individual, device, IP address, or account. In contrast, [mass surveillance](#) entails the interception and monitoring of entire communication infrastructures - such as data cables, networks, or servers - or the purchase of bulk data from third parties, allowing access to vast quantities of unencrypted information. Examples of mass surveillance include NSA's PRISM and XKeyscore programs; or China's national surveillance grid.

Targeted surveillance can be carried out through **device-based surveillance** techniques, where there is a direct intrusion into personal devices to access communications, location, files, and metadata. Methods include spyware/malware (e.g., Pegasus, FinFisher); remote access tools (RATs); or SIM card tracking and IMSI catchers (e.g., Stingrays).

Targeted surveillance can also be deployed through **geolocation and movement surveillance**, where individuals' physical movements are tracked using digital tools, such as GPS and cell tower triangulation, Bluetooth and Wi-Fi tracking, or through mobility data from apps.

Biometric surveillance refers to the collection and analysis of biological data for identification or monitoring - facial recognition; fingerprints, iris scans, voiceprints; DNA databases.

Open-Source Intelligence (OSINT) surveillance is a technique for collection of publicly available information from open sources, in particular social media profiles, news sites, forums, public databases.

1.3 Who is behind the mask?

The global digital surveillance ecosystem has evolved significantly over the past two decades, expanding from largely state-operated mass surveillance systems to a complex, hybrid web of state and corporate actors engaged in both mass and targeted monitoring. Initially dominated by intelligence agencies in the Global North - most notably the U.S. National Security Agency (NSA) - [the ecosystem](#) was exposed by Edward Snowden's 2013 revelations, which unveiled the scale and sophistication of programs like PRISM and XKeyscore. These systems relied on bulk collection of telecommunications and internet data from global users, often in [secret collaboration with major tech companies and intelligence partners](#) (e.g., the UK's GCHQ), under frameworks such as the U.S. Foreign Intelligence Surveillance Act (FISA). The focus was on pre-emptive security and the assertion of national cyber-sovereignty, often at the expense of global privacy rights.

Over time, the surveillance landscape shifted toward targeted, privatized, and commodified forms of surveillance, marked by the rise of commercial spyware. Tools like Pegasus and Paragon gave governments - including those with poor human rights records - access to capabilities previously reserved for elite intelligence agencies. These spyware tools are capable of covertly infiltrating mobile devices, extracting personal data, and activating cameras and microphones, all without the target's knowledge. The targeting of journalists, human rights defenders, lawyers, and political opponents has become a growing concern, highlighted by expert research centres and CSOs such as Citizen Lab, Amnesty International, and Forbidden Stories. Unlike mass surveillance programs, these tools are marketed and exported by private companies in a largely unregulated global surveillance industry.

Law enforcement agencies and military cyber units often employ surveillance for crime prevention and national security. Tools such as Stingray devices (also called "dirtboxes") are used to mimic cell towers and intercept mobile communications. Automated License Plate Readers (ALPR) and facial recognition systems are deployed for public monitoring and crowd control. While these tools are marketed as crime-fighting technologies, they also pose risks to journalists by, among other things, enabling covert tracking of movements or identification at protests or sensitive events.

Today, the surveillance ecosystem is characterized by blurring boundaries between public and private actors, weak global regulatory frameworks, and an expansion of surveillance capabilities across geopolitical lines, including in the Global South. Major tech platforms continue to play an ambiguous role - both as enablers of surveillance through data collection and as 'defenders' of user privacy through encryption and legal challenges. Meanwhile, governments continue to [justify surveillance](#) in the name of national security, public health, or digital sovereignty, often without transparency or accountability. What we are witnessing now is not only a deepening of surveillance capacity, but also its normalization, with the rights to privacy, freedom of expression, and democratic oversight increasingly under threat. A truly accountable global governance model for surveillance remains elusive - raising urgent questions for media freedom, digital rights and justice advocates worldwide.

New cases have also pointed to digital surveillance as a tool of transnational repression: authoritarian regimes are increasingly using surveillance to target journalists, activists, and dissidents beyond their

own borders, including in liberal democracies. For example, Iranian journalists working outside Iran have frequently been [targeted](#) by the Iranian authorities.

While earlier discussions on surveillance centred on mass data collection and domestic infringements of privacy, [new evidence](#) reveals a new geopolitical and extraterritorial dimension: regimes are no longer confined to silencing dissent within their own jurisdictions - they are leveraging spyware, hacking, and digital harassment to suppress expression abroad.

It is important to remember that contemporary surveillance practices are deeply rooted in the exploitation of 'big data' generated through social media platforms. Companies such as Facebook and Google rely on business models that depend on the systematic collection and analysis of user data. Their market value is built on the ability to produce granular insights into users' locations, behaviours, consumer preferences, political views, and social connections. As a result, these platforms are intentionally engineered to optimize corporate surveillance.

Telecommunications providers and major platform companies both contribute to surveillance ecosystems. Telecoms often retain metadata and location logs, which may be made available to governments under lawful interception regimes. Meanwhile, platforms owned by Google, Facebook/Meta, Apple, and others collect extensive personal data such as browsing patterns and social graphs; this data may be accessed by state agencies or fall prey to misuse. Although these platforms sometimes push back against surveillance via encryption or legal contestations, their role in enabling mass data collection remains central.

Mapping Actors of the Digital Surveillance Ecosystem		
The digital surveillance ecosystem is vast and increasingly complex, involving a diverse array of actors operating across public, private, and transnational domains. Understanding who is behind surveillance - and how their roles, tools, and motivations differ - is essential to identifying threats to privacy, press freedom, and democratic accountability. The following table maps the key categories of actors involved in digital surveillance, including state intelligence agencies, law enforcement bodies, military cyber units, private spyware firms, tech platforms, and data brokers. It also highlights the growing entanglement between public and private interests, the role of international intelligence alliances, and the importance of watchdogs and whistleblowers in exposing abuses.		
Actor Type	Role in Surveillance	Methods / Tools
State Intelligence Agencies	Design and operate mass and targeted surveillance systems for national security purposes	Bulk data collection, metadata mining, hacking, signal interception
Law Enforcement Agencies	Use surveillance for crime prevention and investigation	Cell-site simulators, facial recognition, social media monitoring
Military Cyber Units	Conduct offensive and defensive cyber surveillance and cyber warfare	Network intrusion, espionage malware, electronic warfare

Private Surveillance Companies	Develop and sell spyware and surveillance tools to governments and other clients	Spyware (e.g., Pegasus), zero-click exploits, device surveillance
Telecom & Infrastructure Providers	Enable surveillance through infrastructure access and data retention	Network traffic monitoring, lawful interception, data logs
Big Tech Platforms	Collect vast user data that can be accessed by governments or misused	Social media tracking, app data collection, algorithmic profiling
Third-Party Data Brokers	Aggregate and sell personal data from online/offline sources	Browser tracking, location data sales, advertising profiles
Authoritarian Governments	Employ surveillance to suppress dissent, monitor activists and journalists	Internet shutdowns, spyware, social media censorship
Democratic Governments	Use surveillance under legal frameworks, but often with limited transparency or oversight	Data retention, intelligence sharing, predictive analytics
International Intelligence Alliances	Coordinate cross-border surveillance efforts among member states	Metadata exchange, SIGINT sharing, legal cooperation
Surveillance Watchdogs & Whistleblowers	Expose abusive practices and advocate for transparency and accountability	Investigative reporting, leaks, FOI requests, public advocacy

1.4 The digital surveillance market – the big players

The [global commercial spyware sector](#) is estimated at around \$12 billion per year, driven by strong government demand and a lack of regulation. Some of the main producers include:

NSO Group

NSO Group Technologies Ltd. is an Israeli cyber-intelligence firm founded in 2010 by former members of Israel's 8200 intelligence unit. It is widely known for its flagship spyware tool, Pegasus, which can infiltrate iOS and Android devices and is marketed exclusively to [vetted government intelligence, law enforcement, and military agencies](#) under export authorization from Israel's Ministry of Defence. [Pegasus](#) enables covert, remote installation on a target's phone - often via "zero-click" exploits - and grants access to messages, emails, location, recordings, camera feeds, and encrypted app communications. [NSO](#) also sells Phantom, a version tailored for U.S. targets, distributed through its Westbridge Technologies, and [Circles'](#) phone geolocation tools.

While NSO asserts that it does not operate Pegasus or access client-collected data, [recent legal evidence](#) challenges this claim. Lawsuit filings between WhatsApp and NSO include sworn depositions indicating that NSO employees - not clients - manage spyware installation and data extraction.

In 2023, while checking the device of an individual employed by a Washington DC-based civil society organization with international offices, [Citizen Lab](#) found an actively exploited zero-click vulnerability being used to deliver NSO Group's Pegasus mercenary spyware. They referred to the exploit chain as BLASTPASS.

NSO has faced mounting scrutiny. It was added to the [U.S. Commerce Department's Entity List](#) in 2021 (meaning it cannot do business with US companies without specific government approval) and remains under trade restrictions, with [efforts to remove its listing](#) later rejected by authorities. The company has been said to be pushing to be removed from the [list under the Trump administration](#).

The company has also been implicated in a [damages award for unauthorized hacking](#) by a U.S. court. WhatsApp and its parent company Meta sued NSO Group for using WhatsApp's servers to target more than 1,400 users' devices with Pegasus spyware. NSO Group was ordered to [pay more than USD167 million in damages](#) to WhatsApp. During a hearing in the lawsuit, NSO's lawyer publicly identified Mexico, Saudi Arabia and Uzbekistan as clients linked to the [2019 Pegasus spyware attacks](#), marking the first public acknowledgment of NSO's government customers.

In November 2021, [Apple filed a lawsuit against NSO Group and its parent company, Q Cyber Technologies](#). The complaint accused NSO of deploying its Pegasus spyware to infiltrate Apple devices without user consent - employing the so-called FORCEDENTRY exploit, a zero-click method uncovered by Citizen Lab. Apple sought a permanent injunction to bar NSO from using any Apple technology, as well as compensatory and punitive damages, criticizing NSO's tools as "sophisticated, state-sponsored spyware" abused to surveil journalists, activists, dissidents, and academics.

In January 2024, a judge denied NSO's attempt to shift the case to Israel and upheld jurisdiction in the U.S., allowing the lawsuit to proceed. However, in September 2024, Apple filed a motion to dismiss the lawsuit, citing [risks](#) to its core threat intelligence and security infrastructure. Apple argued that continuing litigation could unintentionally reveal critical internal defences and techniques used to combat spyware. Apple also noted that while the suit had weakened NSO's position, the broader commercial spyware landscape had since diversified - meaning a legal victory might have limited industry impact.

Paragon Solutions

Founded in 2019 in Tel Aviv, Israel, Paragon Solutions Ltd. is an Israeli spyware firm co-founded by former Unit 8200 commander Ehud Schneerson and former Prime Minister Ehud Barak, alongside others. Paragon presents itself as a more ["ethical" alternative](#) in the emerging spyware industry, claiming it only sells to democracies that respect international norms.

Paragon's flagship product, Graphite, is a zero-click spyware tool capable of infiltrating mobile devices via vulnerabilities in messaging apps (e.g. WhatsApp, iMessage). It enables access to encrypted messages, location data, microphones, and cameras. Paragon allegedly sells Graphite to [government clients](#) for national security purposes, but it has been found on the phones of journalists, activists and other civil society members in countries around the world in recent years.

In 2024, news outlets reported that a [\\$2 million contract](#) between Paragon and the United States Immigration and Customs (ICE) had been paused and placed under compliance review, due to human rights concerns.

In January 2025, an official with Meta's WhatsApp affirmed Paragon Solutions had targeted its users, including journalists and members of civil society. WhatsApp detected [hacks](#) targeting 90 users in over two dozen countries. In April 2025, a group of [iOS users](#) were notified by Apple that they were targeted with advanced spyware.

In 2025, Citizen Lab confirmed Graphite infections on the devices of [Italian journalists](#) such as Ciro Pellegrino and Francesco Cancellato, as well as activists like Luca Casarini and Giuseppe Caccia. The Italian parliamentary intelligence oversight committee ([COPASIR](#)) acknowledged limited use of Graphite against activists under legal authorisation but has not clarified who targeted Cancellato or others. News reports later indicated that the company had [terminated contracts with clients in Italy](#). Technical analysis by researchers suggests [deployments](#) in Australia, Canada, Cyprus, Denmark, Israel, and Singapore, with possible links to Canada's Ontario Provincial Police.

Gamma Group

Gamma Group is an Anglo-German technology company known primarily for its government-grade surveillance software suite called [FinFisher](#) (also known as FinSpy), developed by its subsidiary Gamma International GmbH.

The FinFisher suite actually consists of a range of intrusion and surveillance tools for both desktop and mobile platforms, including

FinSpy (desktop and mobile versions), which covertly enables [full remote access to target devices](#) - including encrypted communications, webcam, microphone, and files; FinFireWire, FinFly ISP, FinFly USB, FinFly Web, and FinIntrusion Kit, tools for unlocking and infecting devices using advanced delivery methods; and accompaniment by FinTrack Operation Center and FinTraining programs for operational support and user training.

In 2013, Citizen Lab found [command and control servers](#) for FinSpy backdoors, part of Gamma International's FinFisher "remote monitoring solution," in 25 countries: Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam.

In 2019, a number of CSOs filed a criminal [complaint](#) alleging that the CEOs of FinFisher GmbH, FinFisher Labs GmbH, and Elaman GmbH sold the spyware FinSpy to Turkey without the German federal government's authorisation. In March 2022, following the criminal complaint, German authorities seized the company's accounts. Shortly thereafter, FinFisher GmbH and its affiliates filed for insolvency, effectively [ceasing operations](#) under that legal entity. In May 2023, prosecutors in Munich filed [criminal charges against four former executives](#) of the Gamma Group.

Candiru (Saito Tech Ltd., also referred to as Caramel Tsunami)

Based in Tel Aviv, founded in 2014 by Eran Shorer and Yaakov Weizman and chaired by Isaac Zach. Its main product is [DevilsTongue](#) - a sophisticated spyware implant that targets multiple platforms, including Windows, macOS, iOS, Android, and cloud environments. It is delivered through zero-day exploits, bypassing user interaction, and allows full remote control over the target device - it can be used to

compromise Windows systems, enable [browser-based infection](#) in targeted campaigns, and [exfiltrate](#) messages, files, credentials, and even activate the camera/microphone.

The spyware has been deployed in highly targeted operations, predominantly against journalists, human rights defenders, political dissidents, academics, and embassy staff. [Microsoft and Citizen Lab](#) documented at least 100 victims across multiple countries - including Palestine, Lebanon, Turkey, Spain, UK, Armenia, and Singapore. ESET observed watering-hole attacks on websites associated with [Middle Eastern entities](#), injecting JavaScript to deliver browser exploits to users visiting compromised domains. [Avast](#) reported renewed campaigns starting in early 2022, targeting journalists in Lebanon, Turkey, Yemen, and Palestine using a Chrome exploit, suggesting continued operation post-2021.

DevilsTongue was used in the CatalanGate case, alongside the more widely documented Pegasus spyware. The Citizen Lab investigation report released in 2022 identified that 65 individuals connected to the Catalan independence movement were targeted - 63 by Pegasus and 4 by Candiru spyware. These victims included elected officials, members of the European Parliament, legal professionals, activists, and members of civil society, and in [two cases](#), individuals were targeted with both Pegasus and Candiru.

Chapter 2. Digital surveillance – Country overviews

This chapter provides a summary of the 10 country case studies presented in detail in Part II of this report. References and details can be verified in the full accounts found in Part II.

2.1 India

India has steadily built up both mass surveillance infrastructure and targeted spyware capabilities over the past decade. In the early 2010s, major projects like the Centralized Monitoring System (CMS) and NATGRID were launched to give security agencies direct access to telecommunications and centralized databases, raising alarms about unchecked mass interception. At the same time, India began experimenting with commercial spyware. In 2013, researchers at Citizen Lab uncovered FinFisher spyware servers operating on Indian networks, indicating that Indian agencies had obtained the FinSpy malware suite for covert hacking of computers and phones. Leaked emails later confirmed Indian intelligence interest in Italy's Hacking Team spyware; by 2014, the Intelligence Bureau and other agencies were evaluating Hacking Team's Remote-Control System (RCS) tool. These early incursions showed India's willingness to acquire "lawful intercept" malware from abroad to bolster domestic surveillance.

By the late 2010s, India's use of spyware became public with the Pegasus scandal. In 2019, WhatsApp revealed that NSO Group's Pegasus had been used to infect phones worldwide – including at least 121 users in India (journalists, activists, lawyers) over a two-week period. Subsequent investigations confirmed an Indian Pegasus operator active since 2017, codenamed "Ganges," which targeted devices inside India and neighbouring countries. The revelations sparked political uproar: the government was accused of using Pegasus to surveil critics and opponents, though officials issued evasive "non-denial" responses. Civil society petitioned the Supreme Court, which in 2021 appointed a committee to probe the Pegasus use. While that inquiry proceeded, further reporting suggested Pegasus was also used for state-on-state espionage – for example, to spy on senior Pakistani officials in 2019. The Pegasus affair underscored how advanced spyware had become a tool of India's security apparatus, prompting calls for stronger oversight and transparency in surveillance practices.

2.2 Pakistan

Pakistan's authorities have likewise been linked to both domestic spying and falling victim to foreign spyware operations. In 2013, Citizen Lab found FinFisher spyware servers on Pakistani networks, prompting the NGO Bytes For All to file a court petition in Lahore. While the case stalled, a later leak of FinFisher's internal data revealed a Pakistani customer had purchased the FinSpy suite as early as 2010 for roughly €300,000. This evidence strongly suggests a Pakistani intelligence agency was using FinFisher to secretly monitor targets, a claim that authorities neither confirmed nor denied. In 2015, the Hacking Team leaks showed Pakistani intermediaries negotiating with the Italian spyware firm to buy its RCS malware for the National Police and intelligence units. It remains unclear if those Hacking Team deals were finalized, but the outreach demonstrated Pakistan's interest in acquiring cutting-edge intrusion tools. Around the same time, Pakistani activists and journalists reported an increase in phishing and malware attacks. A 2018 Amnesty International investigation uncovered a targeted campaign using fake personas and malicious links to infect the devices of human rights defenders like Diep Saeeda. These

incidents raised concern that domestic agencies or their proxies were deploying spyware against civil society.

Pakistan also became a target of foreign spyware. Notably, in mid-2019, at least two dozen Pakistani senior officials – including defence and intelligence officers – had their phones infected by Pegasus spyware. The sophisticated operation, disclosed by WhatsApp and later confirmed by investigative reporting, appeared to be “state-on-state” espionage. Sources pointed to India as the likely operator behind these Pegasus hacks on Pakistani officials. The Pakistani government quietly probed the breach and even announced plans to develop a secure local messaging app for official use. The Pegasus episode underscored Pakistan’s dual role in the spyware realm – as a perpetrator of domestic surveillance and as a high-profile target of rival state operations. To date, however, Pakistan has seen little accountability: local courts and regulators have not decisively curbed spyware use, and digital espionage against activists and journalists continues to be reported amidst an absence of adequate privacy legislation.

2.3 Kenya

Kenya has rapidly expanded its digital surveillance usage in recent years, blending traditional interception with modern spyware. In the early 2010s, security agencies ramped up intelligence operations ahead of the 2013 elections – including a controversial nationwide filtering system for internet traffic and bulk call monitoring equipment. By 2014, following terrorist attacks like Westgate, the government invested heavily in surveillance infrastructure (such as a city-wide CCTV network with facial recognition) as part of a counterterror strategy. Around the same time, Kenya quietly obtained sophisticated spyware from abroad. In 2015, Citizen Lab discovered FinFisher malware operating on Kenyan systems; the FinSpy server was even registered to “National Security Intelligence,” indicating the National Intelligence Service (NIS) as the user. Leaked Hacking Team emails showed that Kenyan officials negotiated to buy the RCS spyware and even requested Hacking Team’s help to break into journalist Robert Alai’s blog “[Kahawa Tungu](#)” which was known for highlighting corruption in the Kenyan government - a request that was ultimately declined. These revelations confirmed that Kenyan intelligence sought tools to hack devices and surveil dissidents, beyond standard wiretap methods.

By the late 2010s, Kenya’s surveillance appetite extended to mobile spyware and interception gear. The Communications Authority’s attempt to implement a Device Management System (ostensibly to catch counterfeit phones) in 2017 was widely opposed as a mass surveillance strategy, and courts halted the system as a privacy threat. Nevertheless, investigative research identified Kenya as a client of Israel’s NSO Group: a 2018 Citizen Lab scan found a Pegasus spyware operator active inside Kenya. While specific Pegasus targets remain undisclosed, observers note the tool would enable clandestine access to opposition figures’ calls and messages. Additionally, Kenya was found to be using the Circles platform (an NSO affiliate), which exploits telecom SS7 flaws to track phones and intercept calls without malware. In September 2025, [Citizen Lab](#) discovered *FlexiSPY* on devices belonging to filmmakers covering a [BBC documentary](#) on police violence, which allows monitoring of calls, messages, social media, and passwords. Together, these capabilities - FinFisher, Hacking Team’s RCS, Pegasus, and Circles - gave Kenyan authorities a potent arsenal for internal security and surveillance of government critics. Digital rights groups warn that these tools have been deployed under weak oversight, citing Kenya’s increasingly repressive stance toward dissent. Legal challenges (such as the DMS case) illustrate a growing pushback, but as of 2023 the state’s digital surveillance powers continue to expand in scope and sophistication.

2.4 Italy

Italy is both a producer and consumer of advanced spyware technology. Domestically, Italian law enforcement has long been a heavy user of wiretaps under judicial authorization. In the early 2010s, authorities began adopting more advanced hacking tools alongside traditional intercepts. Italy's own Milan-based company, Hacking Team, was a global supplier of spyware (the "Galileo" RCS malware) - and Italian police and intelligence agencies themselves became clients. Internal documents later confirmed that units of the Polizia di Stato and Carabinieri purchased Hacking Team's RCS system to hack suspects' devices. This raised ethical concerns, as Hacking Team had also sold its tools to authoritarian regimes involved in human rights abuses. The issue became widely public when Hacking Team was hacked in 2015, leaking 400GB of emails. The leaks revealed Italian agencies' contracts with Hacking Team and sparked debate about domestic use of "zero-day" spyware without public oversight. Italian officials defended their use of malware as lawful and necessary for fighting organized crime and terrorism, but civil society questioned the lack of transparency and external controls.

After Hacking Team's collapse, other Italian firms filled the void. Milan-based RCS Lab (unrelated to Hacking Team's RCS product) provided interception services and in 2022 was outed as the developer of the "Hermit" spyware, found deployed on phones in Italy and Kazakhstan. Hermit, a sophisticated mobile malware, was delivered in some cases with telcos' collusion - disabling a target's data and pushing a fake app download. The discovery of Hermit on Italian soil raised questions about whether Italian agencies had used it and whether judicial safeguards were in place. Italy also drew scrutiny in the European Parliament's 2022 PEGA inquiry into spyware, with companies like RCS Lab and Tykelab accused of enabling cross-border surveillance. While Italian officials maintain that any surveillance is court-approved, documented cases illustrate the potential for abuse. For example, Citizen Lab mapped Italian government spyware servers on domestic ISPs, and one 2011 case showed a private firm helping police infect a journalist's computer with Hacking Team malware.

Between 2023 and 2025, Italy faced a rare, well-documented spyware scandal inside the EU, centred on the deployment of Israeli-made Graphite (Paragon Solutions) against investigative reporters. Forensics by independent researchers confirmed that the iPhones of Francesco Cancellato (editor-in-chief of *Fanpage.it*) and Ciro Pellegrino (Naples bureau chief) bore the traces of Graphite infections, consistent with zero-click delivery and full device compromise; both had led sensitive investigations into far-right networks and public corruption. A parliamentary security oversight summary (COPASIR) subsequently acknowledged that Italian intelligence services had activated contracts with Paragon in 2023–24 and used the spyware on a limited number of targets under judicial warrants, while denying deliberate surveillance of journalists; nevertheless, the disclosures triggered multiple prosecutorial inquiries (including in Rome and Naples) and, in June 2025, the government terminated the Paragon contract. Press-freedom groups condemned the attacks as a direct threat to source confidentiality, and the episode quickly became a touchstone in European debates over a ban or strict moratorium on mercenary spyware, marking one of the first clear cases of a mature EU democracy being forced to publicly confront the domestic use of hacking tools against the media.

2.5 Serbia

As this report was being completed media [reports](#) exposed the largest documented wave of surveillance in Serbia, including the use of the Pegasus spyware. The victims are believed to include journalists who covered the recent student protest movement.

Serbia has in recent years amassed a considerable array of surveillance tools - both imported and homegrown - which have allegedly been used against journalists and civil society. Throughout the 2010s, Serbian agencies like the Security Information Agency (BIA) and Ministry of Interior quietly procured spyware from abroad. For instance, by 2013 Citizen Lab had identified FinFisher malware servers on Serbian government networks, indicating that Serbia was among the governments using Gamma Group's FinSpy spyware for covert monitoring. Emails from the Hacking Team leak show that as early as 2011, Serbia explored buying Hacking Team's RCS spyware (though a deal allegedly never materialized). Instead, Serbia seems to have turned to other vendors: by 2015, leaked records tied FinFisher deployments to Serbian state security, and by 2017 the Israeli firm Cyberbit was marketing intrusion malware to Serbia. The country also invested heavily in IMSI catchers – devices that mimic cell towers to intercept calls and texts. More than 20 IMSI-catcher units have been imported, including a €2 million system for the police, yet Serbia has no laws explicitly regulating their use. This legal grey zone has raised fears of abuse, such as police using IMSI catchers to surveil protesters without warrants.

By 2020, evidence emerged that Serbia obtained some of the most advanced spyware on the market. Researchers discovered a Serbian operator of the Predator spyware (developed by Intellexa), confirming Serbia as a client of this NSO Group competitor. In parallel, Serbian authorities repeatedly renewed licenses for Cellebrite forensic tools, which can unlock smartphones and extract all data. Amnesty International forensically documented how Serbian police and BIA used Cellebrite to physically install a custom spyware agent (named “NoviSpy”) onto activists' phones during interrogations. NoviSpy, developed in-house by Serbian security, can record audio, steal files and track location - effectively Serbia's own spyware implant. The cumulative effect is a sweeping surveillance arsenal spanning network interception, foreign “mercenary” spyware, and local malware development. Unsurprisingly, multiple high-profile abuses have been alleged. In 2021–2022, at least two Serbian human rights defenders and later two investigative journalists received Pegasus infection attempts, confirmed by Citizen Lab and Amnesty tech labs. The journalists (from BIRN) were targeted via WhatsApp and Viber messages containing Pegasus links - attacks fortunately foiled when they did not click the bait. These were the first confirmed uses of Pegasus inside Serbia, implicating a government client since NSO sells only to states. The Serbian government has neither confirmed nor denied purchasing Pegasus or Predator, but the pattern of targets (pro-democracy activists, critical media) strongly suggests use for domestic political surveillance. Serbian and international NGOs have condemned the “alarming” espionage campaign against civil society, calling for investigations. Thus far, no officials have been held accountable.

2.6 Brazil

Brazil's experience with digital surveillance shows an evolution from conventional intercepts to bold spyware abuses, especially under recent political leadership and currently under investigations. In the early 2010s, Brazilian law enforcement primarily relied on lawful wiretap systems like the homegrown Guardiã platform to monitor calls and data with court orders. Following the 2013 Snowden revelations

(which showed the U.S. NSA spied on Brazil's government), Brazilian authorities grew more conscious of surveillance tools. By 2014, leaked contracts revealed the Federal Police had engaged Italy's Hacking Team to pilot its RCS spyware. The 2015 Hacking Team leaks confirmed Brazil obtained a three-month trial of the Galileo malware, with court authorization to infect 17 targets for 15 days. This made Brazil one of the first democracies in Latin America to use government-grade spyware. The episode raised debate over legal oversight, since a 2015 law allowed sensitive police equipment purchases without competitive bidding (and, therefore, oversight). In response to rising crime and corruption probes (like Operation Car Wash), Brazilian agencies also expanded use of forensics tools: by 2015–2018, federal and state police widely deployed Cellebrite devices to crack seized phones and retrieve encrypted chat data. Although no public evidence showed Brazil purchasing FinFisher, researchers found hundreds of procurement documents indicating steady investment in spyware and cyber-intel training during this period.

A turning point came under President Jair Bolsonaro (2019–2022), when surveillance was weaponized for political ends. Shortly after Bolsonaro's election, Brazil's intelligence agency (ABIN) secretly acquired an Israeli cellular tracking system called FirstMile (made by Cognyte/Verint). FirstMile exploits telecom network flaws to geolocate phones in real time without any device infection or court warrant. Under Bolsonaro's directive, ABIN ran a clandestine program that between 2019 and 2021 conducted over 60,000 location lookups on thousands of phones. Targets included at least 13 journalists, opposition politicians, judges, and even officials deemed disloyal. Internal communications later exposed that agents were profiling reporters' political leanings and movements. This massive spying scheme – essentially a “parallel ABIN” – was carried out with no judicial oversight and in direct violation of Brazilian privacy laws and included 13 journalists among its targets, including Leandro Demori, then executive editor of The Intercept Brasil. A 2025 federal police report concluded that Bolsonaro personally benefited from the illegal surveillance, and multiple former ABIN officials (including its ex-chief and one of Bolsonaro's sons) are under investigation. In addition, Bolsonaro's administration attempted to obtain more offensive spyware. In 2021, the Ministry of Justice launched a million-dollar tender to purchase NSO's Pegasus – a deal from which traditional security agencies were deliberately excluded, reportedly at the behest of Bolsonaro's son, to build another parallel spying capability. Brazilian media revealed that the plan aimed to monitor targets without court orders and outside institutional checks. Ultimately, the Pegasus tender was aborted amid public outcry and NSO's international blacklisting. However, Brazil's military did later admit to buying lesser-known spyware (like Israeli-made Grade/Firefly malware) in 2021 for intelligence use – again, with little transparency.

Brazil's trajectory shows a dramatic misuse of spyware against the media and democratic institutions. Investigations by civil society have detailed how the Bolsonaro government's secret surveillance violated journalists' rights on a large scale, leading to calls for accountability. The Brazilian Supreme Court has since declassified documents on the “parallel ABIN,” and lawmakers are debating reforms to prevent such abuses. The Brazil case underlines that even where legal frameworks exist, political actors can subvert them – leveraging cutting-edge spyware for personal or partisan agendas until robust oversight and penalties are in place.

2.7 Mexico

Mexico is often cited as *ground zero* for spyware abuse, given the extensive targeting of journalists and civil society by state actors. Mexican authorities have a history of buying surveillance tech: they were

early customers of FinFisher (with Citizen Lab detecting FinFisher servers in Mexico in 2013) and Hacking Team (multiple Mexican federal and state agencies appeared in the 2015 Hacking Team leaks as clients). But the most notorious tool in Mexico has been NSO Group's Pegasus. Between 2014 and 2017, under President Peña Nieto, Pegasus was widely deployed against investigative journalists, anti-corruption activists, lawyers, public health advocates, and even the family members of government critics. A landmark 2017 investigation by Citizen Lab and local NGOs (R3D, SocialTIC, Article 19) revealed that at least 76 Pegasus infection attempts were sent to targets including [prominent journalists](#). On 7 March 2023, a joint investigation published by [The New York Times](#) and [Aristegui Noticias](#) reported that the Mexican Armed Forces used NSO's Pegasus surveillance software to spy on the communications between journalists at the newspaper *El Universal*, and human rights defender Raymundo Ramos. Other prominent cases included journalist Ricardo Raphael and a reporter from *Animal Politico*.

The spyware lures were chilling – SMS messages impersonating U.S. embassy officials, emergency AMBER alerts, even personal threats – all containing links to Pegasus exploits. These revelations (the *Reckless* series of reports) sparked outrage in Mexico and internationally. Although the Peña Nieto administration denied wrongdoing, evidence showed the spyware activity closely tracked sensitive investigations into government corruption and human rights abuses. No officials were ever charged in Mexico's Pegasus scandal, even as the spyware's misuse was widely condemned.

Despite the change of government in 2018, Pegasus continued to be used in Mexico. A joint investigation by Citizen Lab, Access Now, and others found that 35 journalists and human rights defenders were infected with Pegasus between 2019 and 2021, i.e. during President López Obrador's term. Notably, a forensic audit found Pegasus on the devices of reporters at *El Faro* and other outlets who were investigating the Bukele government in El Salvador – indicating cross-border spying – as well as on domestic targets examining the Mexican Army's conduct. In late 2022, revelations emerged that Mexico's Army had its own contracts with an NSO affiliate and had deployed Pegasus against at least two journalists and a human rights NGO director, even as the civilian government claimed to have halted use of such spyware. This "Army Spy" scandal showed that military intelligence continued to deploy Pegasus in secret, prompting calls for congressional inquiries and a moratorium on spyware. Meanwhile, NSO Group's legal battles have confirmed Mexico's role as a major client: in a 2025 U.S. court hearing, NSO's lawyer identified the Mexican government as one of the customers behind a 2019 Pegasus campaign that hacked 1,400 WhatsApp users worldwide.

Mexico's case highlights both scale and persistence. Despite years of exposés, there has been no legal accountability within Mexico for the unlawful surveillance. Investigations by the Attorney General's office have lagged or remained opaque, and officials implicated in earlier spyware use (including ex-NSO contract managers in Mexico) have not been prosecuted. However, the continued discoveries have kept up pressure. Mexican and international human rights groups have filed complaints and even involved forums like the IACHR to examine the abuses. Mexico has since passed a data protection law and is discussing a surveillance regulation bill, but enforcement remains uncertain. The Mexican experience underscores the importance of independent oversight; without it, even high-profile revelations of spyware abuse have not, so far, deterred powerful security actors from turning these tools on journalists and civilians.

2.8 El Salvador

El Salvador has emerged as a stark example of authoritarian use of spyware against the media. In a joint investigation dubbed “Project Torogoz” (2022), Citizen Lab and Access Now found that Pegasus spyware was systematically deployed to hack the phones of at least 35 Salvadoran journalists and civil society members between July 2020 and November 2021. The victims included reporters at nearly every major independent media outlet - such as *El Faro*, *Gato Encerrado*, *La Prensa Gráfica*, and others - as well as activists and NGO staff. Forensic analysis showed these Pegasus infections coincided with the targets’ work on sensitive stories about President Nayib Bukele’s administration, including investigations into secret gang truces and government corruption. Citizen Lab identified a Pegasus operator active almost exclusively in El Salvador (codenamed “TOROGOZ”), strongly suggesting the spyware was run by a Salvadoran government entity. While the Bukele government has denied any association with Pegasus, the highly focused nature of the hacking (zeroing in on domestic critics) and NSO Group’s policy of selling only to governments make those denials implausible. In practical terms, the entire editorial teams of some outlets were infected. *El Faro* alone had 22 staff members’ phones compromised over that period. Many of these journalists also faced physical threats and public smear campaigns from officials, creating a climate of fear.

The use of Pegasus in El Salvador has drawn international condemnation. It demonstrates an attempt to silence investigative reporting through espionage. The spyware’s aggressiveness was “jaw-dropping,” researchers noted, in that phones were repeatedly reinfected even after some hacking was exposed. This persistence points to a deliberate strategy to monitor and intimidate the media. Following the revelations, a coalition of organizations (Access Now, Amnesty, Citizen Lab, Frontline Defenders) helped the affected journalists file a petition with the Inter-American Commission on Human Rights, and U.S. lawmakers cited the case when sanctioning the NSO Group. As of 2023, no Salvadoran officials have been held accountable for the spyware campaign. President Bukele - who often labels independent media outlets as “enemies” - has remained defiant, even jokingly referring to himself as the “world’s coolest dictator” while concentrating power. The lack of any credible investigation inside El Salvador (and the expulsion of a critical international anti-corruption mission) means the Pegasus abuses persist in impunity. The El Salvador case underscores the urgency of global action. Without export blacklists, corporate responsibility, and human-rights-based restrictions on spyware sales, authoritarian-leaning regimes can and will acquire these tools to undermine free expression and democratic checks.

2.9 Lebanon

Lebanon’s security agencies have built up a notorious surveillance apparatus, marked by both local innovations and high-profile spyware scandals. As early as 2012, the Lebanese Internal Security Forces (ISF) drew criticism for overbroad data demands - at one point requesting all SMS messages and social media logins of the entire country under the pretext of a criminal investigation. Around that same time, evidence emerged that Lebanese intelligence had acquired sophisticated spyware. Citizen Lab’s research in 2015 revealed that both the General Directorate of General Security (GDGS) and the ISF were running FinFisher malware servers on official networks. In fact, one FinFisher server was traced to an IP range registered to “General Security” (strongly pointing to GDGS) and another to an ISF subdomain. Leaked Hacking Team emails further showed that the Lebanese Armed Forces and ISF negotiated purchases of Hacking Team’s RCS spyware in 2014–2015 - including a live demo where ISF officers were taught how to hack phones via a bug in Angry Birds. By mid-decade, Lebanon had access to multiple commercial

spyware suites, and reports surfaced of activists and bloggers being quietly infected during interrogations by the Cybercrime Bureau.

A series of cyber-espionage campaigns tied to Lebanon were subsequently unmasked. In 2015, cybersecurity firm Check Point exposed “Volatile Cedar,” a long-running operation (since 2012) deploying custom malware dubbed “Explosive.” This campaign targeted organizations in Lebanon, Israel, and beyond, and was likely run by a unit linked to Hezbollah or Lebanese military intelligence. Then in early 2018 the “Dark Caracal” report by EFF and Lookout was released. Dark Caracal was a massive spying program operating out of a GDGS office in Beirut. Investigators found it had stolen hundreds of gigabytes of data from thousands of victims in over 20 countries. The attackers pioneered mobile device exploits, creating fake secure messaging apps (Trojanized WhatsApp, Signal, etc.) to infect Android phones and using malware like “Pallas” and “Bandook” to exfiltrate virtually everything (messages, calls, photos, even live microphone audio). Notably, the Dark Caracal hackers left an open stash of intercepted data online, which allowed researchers to pinpoint their location. By tracing test devices and Wi-Fi networks, the operation was linked to the GDGS headquarters in Beirut - literally mapping the spyware controllers to a specific security agency building. This was one of the clearest cases globally of a cyber-espionage crew tied to a state actor’s physical premises. Lebanese officials issued half-hearted denials - the GDGS chief claimed the agency “didn’t have the capability” for such hacking while a cabinet minister admitted the reports were “not untrue, just exaggerated”. No one was charged or removed; the lack of accountability was noted by rights groups as a “massive espionage campaign” with zero oversight.

Lebanon’s surveillance efforts have not ceased. Reports indicate that after Dark Caracal was exposed, its operators simply adjusted tactics and possibly began offering their services to paying clients abroad. In 2022, EFF found Dark Caracal had resurfaced, spying on dissidents as far as Latin America. Meanwhile, other spyware incidents have swirled around Lebanon - for example, Microsoft in 2021 found that the Israeli firm Candiru’s DevilsTongue spyware had over 100 victims including journalists in Lebanon and the Palestinian territories. Despite periodic public outrage (local NGOs have decried Lebanon’s “Orwellian” surveillance practices) and even legal petitions, the country’s laws lag behind - there is no comprehensive privacy or interception law, and security agencies operate with broad leeway under decades-old statutes. The judiciary has largely avoided tackling cases of digital spying; for instance, no prosecutions followed the Dark Caracal exposure.

As a result, Lebanon remains a space for unregulated surveillance, where domestic agencies and possibly partisan militias leverage spyware to entrench power. This not only endangers Lebanese journalists and activists - it also contributes to a regional market of spycraft, as evidenced by overlapping campaigns (like Volatile Cedar and Iran-linked groups) that use Lebanon as a base or target. The Lebanese case underscores how, absent political will and legal reform, a security apparatus can evolve into a pervasive spying machine that outlasts any one scandal.

2.10 Jordan

Jordan has become a prominent example of spyware being used to stifle civic space, especially through the deployment of NSO Group’s Pegasus. In late 2021, Apple’s notification campaign to Pegasus victims revealed that Jordanian activists and journalists had been targeted, prompting Front Line Defenders and Citizen Lab to investigate. By April 2022, researchers confirmed that the iPhones of at least four Jordanian human rights defenders, lawyers, and journalists – such as Suhair Jaradat - were hacked with

Pegasus between August 2019 and December 2021. Citizen Lab identified two separate Pegasus operators focusing on Jordan - which they nicknamed “MANSAF” (active since 2018) and “BLACKIRIS” (since 2020) - likely corresponding to Jordanian security agencies. The timing of the hacks aligned with periods of unrest and crackdowns in Jordan, including protests by the Teachers’ Syndicate and anti-corruption demonstrations. Despite Jordan’s government publicly denying purchasing Pegasus, the forensic evidence and the domestic focus of the spyware activity strongly implicate state actors. Notably, one of the Pegasus infections occurred in December 2021, after Apple had sued NSO and as the company was facing global scrutiny, underscoring that Jordanian clients continued using Pegasus.

Subsequent research revealed that Pegasus use in Jordan was far more widespread. In 2023, a coalition including Access Now, Citizen Lab, Human Rights Watch, and Amnesty International reported that at least 35 Jordanian civil society figures were targeted by Pegasus from 2019 through 2023. This group included journalists, opposition political activists, NGO leaders, and lawyers. The joint investigation (“Between a Hack and a Hard Place”) even documented repeat infections. The report also noted that Apple’s continued threat notifications (another wave in late 2023) led more Jordanians to come forward, implying the true scale of spyware abuse is likely higher.

Among the key cases of journalists being targeted were:

- [Daoud Kuttab](#): An award-winning journalist and director-general of the Community Media Network (including AmmanNet), Kuttab was targeted by Pegasus at least three times in 2022 and 2023. He was arrested upon arrival at Amman airport in March 2022 shortly after his device was first infected, following a complaint under the country's strict Cybercrime Law.
- [Rana Sabbagh](#): A senior editor for the Organized Crime and Corruption Reporting Project (OCCRP) and co-founder of Arab Reporters for Investigative Journalism (ARIJ), she had both of her phones infected with Pegasus in 2021.
- [Lara Dihmis](#): An investigative reporter for OCCRP who was hacked with Pegasus in June 2022.
- [Suhair Jaradat](#): A journalist found to have been targeted by Pegasus six times in 2021.
- [Hosam Gharaibeh](#): Director of Husna Radio and a morning show host, who had his device infected nine times between 2020 and 2022.
- [Hiba Abu Taha](#): A Palestinian-Jordanian freelance journalist who was arrested in May 2024 and sentenced to one year in prison for an article criticizing Jordanian foreign policy regarding the war in Gaza, under the 2023 Cybercrime Law.

Internationally, Jordan’s use of Pegasus has rung alarm bells. Domestically, however, there has been little response - no parliamentary inquiry or punitive action against those responsible. When the initial cases were revealed Jordan’s government simply stated there was “no evidence” it was behind the hacks, and it later formed a committee that reported it found no misuse (a conclusion widely doubted by observers). Meanwhile, unconfirmed reports hinted Jordan may have also procured Predator spyware around 2021, possibly via brokers, though concrete evidence of Predator use has not emerged publicly. What is clear is that Jordan’s General Intelligence Directorate (GID) and other agencies have a history of surveilling journalists and activists using whatever means available. The Pegasus scandal in Jordan highlights the “accountability vacuum” noted by human rights groups. Despite confirmed abuses of

dozens of victims, no Jordanian officials have been investigated or charged. This lack of recourse, coupled with Jordan's restrictive laws on speech and public order, creates an atmosphere where surveillance technology can thrive as a tool of repression. International attention, including mentions in U.S. State Department reports and discussions in the European Parliament, has so far not pushed Amman to transparency. Jordan represents how an ostensibly stable monarchy can quietly deploy some of the world's most advanced spyware to reinforce its internal security regime, with minimal domestic fallout due to a tight grip on media and civil society.

1. INDIA

Summary

Legal Framework

India's surveillance regime is rooted in colonial-era laws updated for the digital age. The Indian Telegraph Act of 1885 (Section 5(2)) long authorized the government to intercept telephone communications on vague grounds like "public emergency" or "public safety". The Information Technology Act, 2000 (amended 2008) extended interception powers to digital data, allowing government agencies to monitor, decrypt, and block online content in the interests of national security or public order (e.g. IT Act §§69, 69A). Oversight of these powers has traditionally been administrative (executive approvals and review committees) rather than independent judicial control, raising concerns about abuse.

In recent years, India has introduced new legislation: the Telecommunications Act, 2023 was enacted to replace the Telegraph Act, significantly expanding state powers (its broad definitions could even encompass encrypted messaging). Likewise, the Digital Personal Data Protection Act, 2023 – India's first data privacy law – contains sweeping exemptions for government agencies. Under Section 17, authorities may process personal data without consent for reasons of "national security" or "public order," effectively excluding surveillance activities from the law's protections. These developments, coupled with the lack of a statutory framework governing India's intelligence agencies, have left significant gaps. Critics warn that while India now has privacy and data protection statutes, their broad exceptions for state surveillance and the absence of an independent oversight body risk undermining the fundamental right to privacy recognized by India's Supreme Court.

Case Law

Indian courts have incrementally built safeguards against arbitrary surveillance. In the landmark *PUCL v. Union of India* (1997) case, the Supreme Court held that phone tapping without proper procedure violates the constitutional right to privacy and laid down detailed guidelines. For example, requiring a senior Home Ministry official's authorization, a fixed interception duration, and a review by a Cabinet Secretary-level committee. This framework aimed to check rampant wiretapping by ensuring accountability. Two decades later, *K.S. Puttaswamy v. Union of India* (2017) elevated the right to privacy to a fundamental right, with the Supreme Court emphasizing that any surveillance measure must be lawful, necessary, and proportionate. Since then, courts have scrutinized surveillance practices more closely. Notably, High Courts have suppressed intercept evidence obtained without adhering to statutory safeguards (e.g. the 2019 *Vinit Kumar* case barred illegally intercepted phone calls from use in trial). In response to revelations that Pegasus spyware had been used to monitor journalists and activists, the Supreme Court in 2021 appointed an independent technical committee to investigate the allegations. This was a sign of judicial concern, though a final ruling on that matter is pending. Additionally, the Supreme Court has curbed allied practices that facilitate surveillance. In *Anuradha Bhasin* (2020) it demanded that internet shutdown orders (often used for security reasons) be published and time-limited, bolstering transparency. Overall, Indian jurisprudence now insists that surveillance adhere to constitutional standards. Any interception must have legislative backing and stringent procedural

safeguards, even as the courts grapple with new technologies (encryption, mass data mining) that test these principles in practice.

1.1 Deployment

Early 2010s: Laying a Foundation for Mass Surveillance

In the wake of the 2008 Mumbai attacks, India embarked on [ambitious internal security projects](#) that would vastly expand its digital surveillance capacity. In 2009 the government launched the Crime and Criminal Tracking Network and Systems (CCTNS) to interlink 15,000 police stations nationwide and digitize records of First Information Reports (FIRs), investigations, and charge sheets. By creating a searchable national crime database, CCTNS aimed to enable data sharing among state police forces and central agencies like the Intelligence Bureau (IB) and Central Bureau of Investigation (CBI). Around the same time, planners conceived the National Intelligence Grid (NATGRID), a counter-terrorism database that would fuse 21 disparate databases (e.g. air travel, bank accounts, phone records) into a single system accessible by 10 authorized agencies (including IB, the Research & Analysis Wing (R&AW), CBI, and Enforcement Directorate). The vision was to allow intelligence and law enforcement to swiftly “profile” suspects by querying consolidated personal data – a step toward integrated mass surveillance.

Another cornerstone was the [Centralized Monitoring System \(CMS\)](#), first proposed in 2011 and quietly approved by the Cabinet Committee on Security. CMS was designed to centralize the interception of all telecommunications and internet traffic in India. Prior to CMS, agencies had to request intercepts from telecom operators on a case-by-case basis; CMS instead would give government monitoring centres direct access to telecom networks, effectively bypassing service providers. The rollout began in April 2013, with plans to eventually monitor all phone calls, SMS, and internet use in real time. Human Rights Watch and Indian civil society sounded alarms that such sweeping surveillance powers, introduced without public debate or new privacy safeguards, could gravely threaten privacy and free expression. India lacked a dedicated privacy or surveillance law at the time, relying instead on colonial-era statutes (the 1885 Telegraph Act) and broad provisions in the Information Technology Act 2008 to govern interceptions. An expert group led by Justice A.P. Shah warned in 2012 that the legal regime was “non-transparent, prone to misuse” and inconsistent on checks and oversight. Critics noted that CMS was created without parliamentary approval or independent oversight, sparking calls for the government to clarify which agencies would use it and under what authorizations. In short, by the early 2010s India was building the legal and technical structure for both targeted interception and mass surveillance, but the rapid deployment of these capabilities far outpaced the development of transparency or accountability mechanisms.

2013–2015: First Incursions into Spyware – FinFisher and Hacking Team

As India ramped up domestic surveillance infrastructure, its security agencies also began experimenting with commercially available spyware for more penetrative targeted monitoring. An important revelation came in 2013 when the University of Toronto’s Citizen Lab uncovered FinFisher spyware command-and-control servers on Indian networks. FinFisher (also known as FinSpy) is a sophisticated “lawful intercept” malware suite sold exclusively to governments by the UK/German company Gamma Group. It can covertly take complete control of a target’s device – bypassing antivirus, siphoning files and

passwords, monitoring Skype calls, and even activating webcams and microphones. Notably, [FinFisher](#) often infects targets by tricking them into installing fake software updates or clicking trojanized files. The Citizen Lab scan identified FinSpy servers in 25 countries, with India marked among the most active (ranked 3 out of 6 on a scale of FinFisher server activity). This strongly indicates that one or more Indian government agencies obtained Gamma's spyware and were operating it on Indian soil. While the specific agencies were not named, the findings implied that Indian law enforcement or intelligence had begun using FinFisher to hack into target computers and phones, potentially against domestic dissidents or criminals, by 2012–2013. The news caused disquiet among privacy advocates, coming on the heels of the Snowden leaks about global NSA surveillance. Observers noted that FinFisher's success underscored how "harmless" metadata can be weaponized. Modules like FinFly Web/ISP can use basic network metadata (IP addresses, browsing habits) to inject spyware into downloads or web pages a target visits. So even before the term "Pegasus" was known in India, the state had access to tools that could surreptitiously infect devices and harvest even encrypted communications.

Around the same period, India's security apparatus explored other hacking tools. In July 2015, a major leak of internal emails from Italian spyware vendor Hacking Team (published via WikiLeaks) exposed the extent of India's interest in its flagship Remote Control System (RCS) spyware. The leaked correspondence revealed that R&AW – India's foreign intelligence agency (referred to as CABSEC, under the Prime Minister's Office) – was one of Hacking Team's clients. As early as 2011, Hacking Team executives travelled to India to demo their malware capabilities to officials. An August 2011 email from an intermediary (Nice Systems) to Hacking Team noted that *"CABSEC... are already a customer of ours... I will prepare and update about all opportunities"*, suggesting R&AW had bought other surveillance solutions and was evaluating Hacking Team's offer. By 2014, interest in Hacking Team's hacking tool had broadened. A leaked February 2014 email cited R&AW, the Intelligence Bureau (IB) (domestic intelligence), and the National Investigation Agency (NIA) as eager to join a webinar about the RCS product (with the National Technical Research Organisation, NTRO, likely advising). Hacking Team's RCS spyware, much like FinFisher, enables stealthy intrusion into computers and mobile devices, allowing agents to intercept calls, copy files, read emails, or even activate device microphones. The leaks showed Indian officials framing such purchases as necessary for "lawful interception against terror outfits," stressing that intelligence collection is clandestine by nature. While the government never officially confirmed these dealings, the Hacking Team leaks provided concrete evidence that Indian agencies were actively procuring cutting-edge spyware and intrusion services on the global market. Indian media reports even noted Hacking Team's staff had conducted on-site demonstrations for a [state police cybercrime unit in Tamil Nadu in 2011](#).

Technologically, the mid-2010s also saw India augmenting its bulk surveillance toolkit. By 2014 the Defence Research and Development Organisation (DRDO) had developed NETRA (Network Traffic Analysis), an internet surveillance system aimed at monitoring online communications in real-time. NETRA (meaning "eye" in Sanskrit) was publicised as India's answer to the NSA's PRISM program. NETRA nodes installed at major ISPs can automatically detect and capture internet traffic containing certain flagged keywords (for example, terms like "attack" or "bomb" in emails, social media, VoIP calls, etc.). In early 2014, the government revealed plans to deploy NETRA widely, with up to 1,000 ISP-level surveillance "nodes", each storing 300 GB of intercepted data. The system was developed by DRDO's Centre for Artificial Intelligence and Robotics and tested by units of the IB and Cabinet Secretariat (i.e. R&AW). [NETRA can even monitor voice traffic over services](#) like Skype and Google Talk. While pitched as

a counterterrorism necessity, the prospect of such broad content filtering raised obvious concerns. An Economic Times report from that time highlighted the paltry 300GB per node storage cap as laughably small given India's population, suggesting the program's scale might later grow. Nonetheless, by late 2014 NETRA was being integrated alongside CMS and existing Lawful Intercept & Monitoring systems to bolster the state's capacity for mass interception of internet and telephone communications. This convergence of mass surveillance architecture (CMS, NETRA, NATGRID) with targeted spyware capabilities (FinFisher, RCS) by the mid-2010s meant that Indian authorities had an expanding menu of digital surveillance tools at their disposal, largely in the shadows and absent specific legislation or oversight.

Late 2010s: Surveillance Expands Amid Political Controversy and Legal Challenges

By 2017–2018, India's use of digital surveillance was accelerating, and cracks were beginning to show in the form of public controversies and court battles. The year 2017 was especially critical. In July 2017, Prime Minister Narendra Modi made an historic visit to Israel and, as later emerged, high-end spyware was on the agenda. Investigative reporting by The New York Times revealed that India acquired the [NSO Group's Pegasus spyware in 2017](#) as part of a roughly \$2 billion package deal with Israel that also included advanced missiles. Pegasus is an offensive cyber weapon that can consistently crack the encryption of any iPhone or Android, giving full access to calls, messages, microphone and camera. While the Indian government kept silence on these allegations, the NYT's article (published in 2022) indicated that the warming of India-Israel ties coincided with New Delhi securing one of the world's most powerful spyware systems. Notably, an earlier Citizen Lab study in 2018 had already pointed to an Indian Pegasus operator active since mid-2017. The report identified a Pegasus operator codenamed "Ganges" that was infecting phones in India and [neighbouring countries](#), with data indicating most of its targets were inside India. Therefore, well before the Pegasus scandal broke publicly, technical evidence suggested that Pegasus was being deployed within India by late 2017, presumably by a government client of NSO. This set the stage for what would become a dispute between the government's secretive surveillance activities and the country's legal and democratic institutions.

2017 also saw a landmark judicial assertion of privacy rights. In August that year, the Supreme Court of India delivered the *K.S. Puttaswamy* judgment, unanimously affirming privacy as a fundamental right under the Constitution. In that decision, the Court specifically warned of the [dangers of unchecked surveillance in the digital age](#), noting that "*technology has permitted surveillance in ways that are unimaginable*," and that any encroachment on privacy must satisfy necessity and proportionality tests. The judgment laid out a three-fold requirement for any law that restricts privacy: it must have a legitimate aim, be backed by law, and be proportionate (minimal intrusion). This pronouncement came partly in response to concerns over Aadhaar (the biometric ID program) but also reflected growing unease about India's widening surveillance net. The Court's recognition of privacy set a new legal benchmark and by implication put schemes like CMS and NATGRID on notice that they operated in a legal grey zone. However, implementing this principle would prove challenging.

Meanwhile, the government continued to propose new surveillance initiatives, sometimes provoking public backlash. In mid-2018, the Ministry of Information and Broadcasting sought to establish a "Social Media Communication Hub" in the form of an outsourced monitoring centre to analyse and report on all trending topics and conversations on social media across India's vast user base. The tender documents explicitly called for technology to collect digital media chatter from all platforms, build a 360-degree

profile of individuals creating buzz, and monitor their past conversations. This project immediately drew legal challenges. Trinamool Congress MP Mahua Moitra filed a lawsuit in the Supreme Court, after which Justice D.Y. Chandrachud stated in open court that *"If the government starts tapping WhatsApp messages, we will be moving towards a surveillance state."* The Attorney General, perhaps sensing the Court's tendencies, informed the justices on August 3, 2018 that the Social Media Hub would be withdrawn. This episode was a rare instance of a proposed mass surveillance tool being stopped in its tracks by public scrutiny. It showed that, at least in the courts, there was growing sensitivity to overt surveillance overreach.

Later that same year, however, in December 2018, the Ministry of Home Affairs issued a notification naming 10 central agencies authorized to intercept, monitor, and decrypt "any information" on any computer resource under the IT Act. The list ranged from the IB and R&AW to the Enforcement Directorate, tax authorities, NIA, CBI, and even the Delhi Police. Although officials insisted this was merely a restatement of existing powers (noting these agencies had been empowered since 2011), the order was widely reported as the [government giving itself "blanket snooping" authority](#). Opposition leaders accused the ruling party of creating a surveillance state, and multiple petitions were filed in the Supreme Court alleging that the notification violated the fundamental right to privacy. In early 2019 the Supreme Court issued notice to the government, seeking its response to these challenges. The Home Ministry scrambled to clarify that each interception still requires a case-specific approval by the Home Secretary and that no new powers were conferred. Nonetheless, the episode underscored the climate of mistrust. The public and political opposition were now openly questioning the scope of government surveillance, and the judiciary was drawn into arbitrating the balance between national security and individual privacy. Notably, around this time the government also operationalized the [National Cyber Coordination Centre \(NCCC\)](#) (in 2017) as an internet traffic monitoring "fusion centre" under CERT-In, further enhancing real-time scanning of web traffic for threats. In sum, by the end of the 2010s India had a dense matrix of surveillance capabilities, from database fusion (NATGRID), to centralised lawful intercept (CMS), to social media monitoring (proposed SMCH), to state-of-the-art spyware (FinFisher, Hacking Team, Pegasus), but each advance was increasingly met with pushback from civil society and the courts calling for adherence to constitutional rights.

2019: Pegasus Targets Revealed and the Spyware Scandal Erupts

2019 was the year India's use of Pegasus was confirmed. In late October, WhatsApp (owned by Facebook) announced that it had discovered a vulnerability in its app being exploited by NSO Group's Pegasus to infect phones, and that 1,400 users worldwide had been targeted in a two-week period. Among those targeted were 121 users in India, the second-highest number in any country. A subsequent lawsuit WhatsApp filed in a U.S. court indicated these targets included Indian journalists, human rights activists, lawyers, and opposition figures. In response, prominent Indian individuals came forward to say they had received WhatsApp alerts that their phones were likely hacked. For example, at least two dozen Indian activists and lawyers connected to sensitive cases (such as those representing Dalit and tribal rights) were identified in media reports as Pegasus targets. This initial Pegasus exposure immediately raised questions concerning who in India ordered this snooping. NSO insists it sells Pegasus only to governments. Thus, suspicion fell on Indian state agencies. Opposition parties, led by the Congress, demanded accountability, with senior leaders alleging the [government had used Pegasus](#) to spy on political opponents. In November 2019, members of Parliament and civil society petitioned the Supreme Court for an independent inquiry.

The government's response at the time was evasive and defensive. The IT Minister acknowledged the WhatsApp breach and professed concern for citizens' privacy, but when pressed in Parliament and RTI queries on whether the government or any of its agencies had purchased Pegasus, officials repeatedly refused to confirm or deny. In one affidavit, the Ministry of Home Affairs claimed it had "no information" on any Pegasus procurement. Effectively, the official line was neither acceptance nor outright denial, a stance criticized as a "non-denial denial" that only fuelled suspicions. Meanwhile, further technical evidence of Pegasus operations in India emerged. In December 2019, The Guardian reported that the earlier analysis of the WhatsApp attack had uncovered a possible India-Pakistan espionage angle, with several Pakistani officials' phones targeted, potentially by the Indian operator of Pegasus. The Guardian cited sources suggesting India could have used Pegasus for "state-on-state" spying, given many Pakistan defence officials were hit. While unconfirmed, this hinted that Pegasus might have been used both internally (against journalists/ activists) and externally (against foreign targets) by Indian entities. The Citizen Lab also publicly identified an Indian Pegasus operator active in 2019, which it nicknamed "Aggah" or "Ganges," bolstering the case that Indian agencies were behind the wave of infections.

2019 also witnessed another case of targeted digital surveillance in India, unrelated to Pegasus but equally chilling. In June 2019, police arrested a group of human rights activists and lawyers – the [Bhima Koregaon](#) case – accusing them of fomenting violence and plotting against the state. Over the next year, defence lawyers raised the claim that incriminating documents found on the accused's laptops were planted by malware. In 2020–21, forensic analysts from Arsenal Consulting (a US-based firm) examined copies of the defendants' hard drives. Their reports, made public in early 2021, revealed a sophisticated hacking campaign had infiltrated the activists' computers for months, depositing dozens of fabricated letters that the police later cited as evidence. One defendant, Rona Wilson, had an attacker [gain access](#) via a phishing email and then use a tool called NetWire (a remote access Trojan) to secretly place documents in his folders.

84-year-old Father Stan Swamy had his computer compromised for nearly 5 years (2014–2019) until the night it was seized by authorities, with the hacker planting files in a hidden folder and even removing traces of the intrusion just hours before the police raid. Arsenal's digital forensic evidence was unequivocal that these activists were "*targeted and framed*" by an external hacker. Furthermore, Citizen Lab and Washington Post reporting later found overlaps between this hacking operation (dubbed "ModifiedElephant" by security researchers) and Indian law enforcement, strongly suggesting state sponsorship. Some of the Bhima Koregaon accused were also selected as Pegasus targets in the same timeframe. The Pegasus Project would later show that at least nine phone numbers linked to the arrested activists were in an NSO client's targeting list. This convergence of evidence suggests state agencies (or operatives aligned with them) deploying multiple kinds of spyware/malware to surveil and implicate human rights defenders. The public reaction to these revelations was one of outrage and deep concern. Domestic and international groups, including the UN High Commissioner for Human Rights, called for the release of the activists and an investigation into the malware planting. The [Bhima Koregaon case](#) became an illustration of how digital surveillance tools can be used not only to watch, but to subvert justice by fabricating evidence. It added another layer to the surveillance debate in India: beyond privacy violations, the direct persecution of dissidents through hacking.

2020–2021: The Pegasus Project and Its Fallout

The Pegasus issue exploded into a full-blown scandal in July 2021 with the publication of the Pegasus Project investigations. This was a global collaborative exposé by media outlets (including The Wire in India, Washington Post, Le Monde, The Guardian, and others) coordinated by Forbidden Stories and Amnesty International's Security Lab. The [Pegasus Project](#) revolved around a leaked list of 50,000 phone numbers selected as candidates for Pegasus surveillance by various NSO clients, and forensic analysis of dozens of phones to confirm infections. The revelations in India were substantive: the leaked data indicated that over 1,000 Indian phone numbers appeared on the Pegasus targeting list, far more than the 121 from the 2019 WhatsApp case. Those numbers included the leading Indian civil society representatives, at least 40 journalists from nearly every major media outlet, civil rights activists, lawyers, academics, businessmen, election commissioners, and opposition politicians. The list also contained the numbers of top political figures: Rahul Gandhi (leader of the main opposition Congress party) was identified as a potential target, as were his close aides. Prashant Kishor, a prominent election strategist for opposition campaigns, was forensically found to have been infected. A sitting Union Minister (Ashwini Vaishnaw) and a Supreme Court staffer who had accused the then-Chief Justice of harassment were on the list. The [forensic analyses](#) by Amnesty's lab confirmed Pegasus infections on the phones of Siddharth Varadarajan (founder of The Wire – see box below), his colleague MK Venu, journalist Sushant Singh and others. In many cases, the timestamps of Pegasus spyware activity coincided with sensitive periods. For example, Kishor's phone was infected in 2021 during heated state elections where he was strategizing against the ruling party.

Never before had there been such concrete evidence of Indian journalists and opposition leaders coming under intrusive surveillance by spyware. The fact that Pegasus is a “zero-click” tool (requiring no action by the target) meant even the most tech-savvy individuals had no defence once their number was selected. Media reports described Pegasus as akin to a “cyber-weapon” turned inward on the country's own institutions of democracy. Opposition parties united in protest, staging parliamentary walkouts and demanding the resignation of officials involved. Through July and August 2021, the Pegasus issue paralyzed Parliament's monsoon session, with the government stonewalling all questions. When pressed, ministers fell back on the refrain that no illegal surveillance is conducted and that any interception is done as per law, without confirming or denying Pegasus usage. The heavy involvement of Amnesty and foreign media in exposing Pegasus allowed the government to cast some doubts on the findings' credibility, but the technical evidence was solid. It became clear that only a government entity in India would have the motive and the means (as an NSO client) to mount such widespread surveillance on journalists, activists and political opponents.

Faced with litigation – multiple lawsuits were filed by Pegasus targets and others in the Supreme Court – the judiciary stepped in. In October 2021, the Supreme Court of India, in a strongly worded order, appointed an independent Technical Committee to investigate the Pegasus allegations. The Court rejected the government's offer to have an internal inquiry and criticised the state for refusing to clearly answer whether it had obtained Pegasus, citing national security to “evade questions”. The Chief Justice famously wrote that “the mere invocation of national security doesn't render the court a mute spectator” and that indiscriminate surveillance could not be allowed. The country's highest court implicitly acknowledged the gravity of the claims and the inadequacy of existing oversight. Over the next several months, the Technical Committee (assisted by cybersecurity experts) collected devices from dozens of petitioners and examined them for traces of Pegasus. In its interim communication, the

committee noted that the Government of India “did not cooperate” fully with the investigation. By August 2022, the committee submitted its report to the Supreme Court. While the full report remains sealed, the Supreme Court’s summary stated that Pegasus was not conclusively found on the 29 phones examined, though some showed malware infections; importantly, the Court highlighted the government’s stonewalling and said the lack of cooperation was not conducive to discovering the truth. Legal analysts suspect that without open acknowledgment from the government or NSO, the committee faced hurdles in attribution, since Pegasus is designed to be stealthy and can self-delete.

Despite the committee’s muted findings, the Pegasus investigation had already altered public discourse. It confirmed that India’s surveillance apparatus now unquestionably included elite hacking tools normally associated with espionage against terrorists or hostile states, but which were turned inward against members of its free press and democratic opposition. Internationally, India’s image suffered in press freedom indices, with watchdogs citing [Pegasus](#) as evidence of declining democratic space. The European Parliament and others referenced India in global discussions on spyware abuse. Within India, the [episode invigorated digital rights activists](#), who led petitions for the reform of surveillance legislation, pending since the 2018 MHA notification.

There were calls for updates to the Telegraph Act and IT Act rules to create stronger oversight (such as independent judicial panels for intercept approvals) and for a robust data protection law that would not exempt government surveillance. At the time, the draft Personal Data Protection Bill included broad national security exemptions for government agencies, which drew criticism that it would legalize mass surveillance rather than restrain it. The Pegasus fallout so far has not yielded an official admission or accountability. But it has clearly galvanized public awareness of digital surveillance.

2022–2025: Continuing Revelations, New Evidence, and Ongoing Debates

In the years following the Pegasus Project, investigations have continued to shed light on India’s use of spyware and the extent of its digital surveillance activities. In January 2022, as mentioned, the New York Times report explicitly named India as a client of NSO Group and Pegasus as a key item in a 2017 [India-Israel defence deal](#). This external confirmation reignited political controversy domestically. The opposition seized on the [NYT report](#) to accuse the government of lying to Parliament and demanded a new inquiry. The government’s response remained a flat “no comments”, neither confirming the purchase nor addressing why it had earlier denied unauthorized surveillance. With the Supreme Court committee’s findings not leading to further action, the issue moved into the arena of public opinion and international scrutiny.

On a parallel track, the [Bhima Koregaon surveillance case](#) saw significant developments. In 2022, Arsenal Consulting released additional reports (their third and fourth in the series) extending the analysis of the NetWire malware operation. Father Stan Swamy, one of the jailed activists, died in custody in July 2021 at age 84, before the evidence of his framing fully came to light. In December 2022, *Washington Post* and Arsenal revealed Swamy’s computer had been hacked for 5 years straight, making him likely the longest-known victim of such a hacking campaign. These reports reinforced calls by UN experts and rights groups for the remaining defendants to be released and for an independent probe into who orchestrated the malware attack. In one report, Wired found clues linking the digital fingerprints (like IP addresses and server infrastructure) of the “ModifiedElephant” hacker to an Indian police jurisdiction. While the government has neither acknowledged nor investigated these claims, they remain a cloud

over India's criminal justice system. The case is now frequently cited by scholars as an example of "digital evidence tampering" used to imprison dissenters.

By late 2023, fresh evidence emerged that Pegasus infections in India had not ceased. In December 2023, Amnesty International and The Washington Post revealed that at least two Indian journalists were targeted with Pegasus as recently as 2023. One of them, The Wire's Siddharth Varadarajan, had actually been a victim back in 2018 (something confirmed by forensic analysis), and now in October 2023 his iPhone was hit again by a Pegasus zero-click exploit. Another target was an editor at OCCRP (a global network of investigative journalists) who received an Apple alert in 2023 and upon investigation his device showed evidence of an attempted Pegasus infection via the latest BLASTPASS exploit in iMessage. These findings indicate that India (presumably its agencies) is either continuing to use Pegasus under an existing contract or has acquired similar spyware from other vendors, even after the 2021 scandal. Amnesty noted that more than 20 Indian journalists and opposition politicians got Apple's "state-sponsored attacker" warnings in 2023, suggesting a broad targeting campaign. Reports in Indian media have hinted that the government, unable to buy Pegasus updates due to the NSO controversy, has been shopping for alternative spyware from companies in countries like Spain or Italy. In 2022 there were rumours of India evaluating spyware from competitors (some names floated include Cytrox's "Predator" or Candiru's tools), though details are scarce.

Public and legal reactions in this period have been mixed. On one hand, there is a sense of surveillance fatigue, since repeated revelations have not led to any prosecutions or official admissions in India. The ruling government has faced relatively little electoral fallout over these issues, partly due to the complex technical nature of the story and the hyper-partisan environment (supporters accept official denials, opponents assume the worst, and the needle of accountability scarcely moves). On the other hand, civil society has not relented. The Internet Freedom Foundation (IFF) and others have ongoing petitions in the Supreme Court seeking comprehensive surveillance reforms, including striking down or reading down laws that enable mass interception without oversight. They argue that India's current framework – executive authorizations under the Telegraph Act/IT Act with only a perfunctory review committee, as detailed below – fails the proportionality test laid out in the Puttaswamy case. These petitions were tagged with the Pegasus files and remain pending. Meanwhile, in August 2023, the government passed a new Digital Personal Data Protection Act, but controversially exempted government agencies from most provisions in the name of national security, which critics say effectively gives legal cover to surveillance operations. A draft Telecom Bill is also under consideration that would formally legalize interception of communications with even fewer checks. Each of these legislative moves has been opposed by privacy advocates citing the [Pegasus episode](#). See below the sub-section on Indian legislation for further details.

Internationally, India's use of spyware has drawn increasing scrutiny. In 2023, an EU Parliament committee invited Indian Pegasus victims to testify as part of its [investigation](#) into Pegasus abuses globally. In the US, lawmakers referenced India when lobbying for sanctions on [NSO Group](#). Yet, India has aligned with other governments to resist a ban on spyware. In UN discussions, it has emphasized the [need for such tools for security](#) and has not supported a moratorium.

Siddharth Varadarajan

On 23 Aug 2023, Mangnale's iPhone 13 Pro (running iOS 16.6) was targeted with Pegasus using a zero-click chain later dubbed BLASTPASS by Citizen Lab. He

received Apple's state-sponsored alert in Oct 2023; Amnesty's forensic analysis was published 28 Dec 2023. Siddharth Varadarajan is a journalist, founding Editor of The Wire. Varadarajan's iPhone was previously infected with Pegasus in April 2018, during the period documented by the 2021 Pegasus Project. In October 2023, he received Apple's "state-sponsored attackers" alert and Amnesty Security Lab's forensics found fresh targeting consistent with Pegasus on 16 Oct 2023. The targeting coincided with Mangnale's work on [OCCRP's Adani investigations](#) into alleged stock manipulation via opaque offshore funds, published 30-31 Aug 2023. ([Adani](#) has denied wrongdoing; Indian regulators said they were examining the claims.)

- **Technology used:** A two-stage zero-click exploit chain combining HomeKit interaction and iMessage delivery of ".pkpass" attachments that embed a malicious WebP image.
- **How the attack worked (intrusion chain):** Amnesty documented bursts of homed (HomeKit) crashes, followed by "sample.pkpass" files arriving via iMessage. Parsing those files (inside Apple's BlastDoor sandbox) triggered further crashes; the embedded WebP image exploited CVE-2023-4863 to attempt code execution and sandbox escape. Amnesty's review of the device's HomeKit logs shows the same attacker-controlled Apple ID interacting with Varadarajan's iPhone that was used to target Anand Mangnale, a step consistent with a two-phase chain (HomeKit + iMessage) described in recent Pegasus operations. The phone was running iOS 16.6.1, which was not vulnerable to the BLASTPASS chain that Amnesty observed in Mangnale's case. [Amnesty](#) found no evidence of a successful compromise in October 2023, suggesting reconnaissance/fingerprinting prior to payload delivery.
- **Evidence collected:** HomeKit interaction entries on 16 Oct 2023 tied to an attacker iCloud address; correlation to Amnesty's broader telemetry of renewed Pegasus activity focused on India (observed since June 2023).
- **Attribution assessment (who was behind it):** [Apple's alert](#) classified this as a state-sponsored threat. NSO, as already mentioned, sells only to government clients. Indian authorities have neither confirmed nor denied use, and declined to fully cooperate with a Supreme Court-appointed technical committee that investigated Pegasus in 2021–2022; its technical report remains unpublished. This leaves no official domestic accountability while keeping state operator the most plausible hypothesis.
- **Forensics & disclosure:** Amnesty (with Washington Post) published results; NSO issued a standard statement about vetted government clients and safeguards.
- **Government response:** Instead of acknowledging potential misuse, officials publicly [questioned Apple](#) and said they would "investigate" Apple's notifications. No transparent probe of Pegasus use has been announced.

- **Mitigations:** Apple patched BLASTPASS-related CVEs earlier in September 2023 and advises high-risk users to enable Lockdown Mode, which Citizen Lab and Apple say blocks this attack chain. (Varadarajan’s device was already on the patched iOS during the October attempt.)
- **Actions Taken:** Victims and civil society filed petitions in the Supreme Court of India, urging an inquiry into the Pegasus abuses. In October 2021, the Supreme Court appointed an [independent technical committee](#) to investigate. The committee examined devices (including Varadarajan’s) and submitted a report in 2022. Journalists also worked with international media (the Pegasus Project) to publicize the abuses, spurring public outrage and parliamentary questions.
- **Outcomes/Responses:** The Supreme Court’s inquiry confirmed the presence of malware on some phones (at least 29) but noted the government’s non-cooperation. The Court has not made the full report public, citing national security. Nevertheless, the [investigation](#) itself was a milestone. It led to greater public awareness and pressure. Internationally, NSO Group was blacklisted by the U.S. in 2021 for enabling such surveillance. While no [officials in India](#) have been held accountable yet, the case prompted calls for stronger surveillance oversight and data protection laws.

1.2 Legal Framework

Norms

The Indian Constitution of 1950 does not provide the right to privacy expressly under any of its provisions. The Right to Privacy has been recognized, however, as a fundamental right explicitly under “Article 21 (Right to Life and Personal Liberty)” through several [judicial pronouncements](#) such as *Kharak Singh v. State of U.P.*, *Govind v. State of M.P.*, *R. Rajagopal v. Union of India*, *Justice K.S. Puttaswamy (Retd) v. Union of India*, which will be further detailed below.

The foundation of surveillance laws in India backdate to British period, with the [1885 Indian Telegraph Act](#), which gave the government power to intercept “on the occurrence of any public emergency” or “in the interest of public safety,” on limited grounds (sovereignty, security of the State, public order, etc.). This was the core telephone-tapping power for over a century.

In 2000, the Information Technology (IT) Act was passed to serve as the primary law governing cybersecurity, digital surveillance, and data privacy (amended in 2008). It grants the Central and State Governments broad powers under Section 69 to intercept, monitor, or decrypt information for national security and public order. Section 69A authorizes the Central Government to block public access to online content, with penalties for non-compliance including imprisonment. Section 69B allows for the collection and monitoring of traffic data to bolster cybersecurity and prevent digital threats. Additionally, Section 80 empowers government officers to search and arrest individuals without a warrant if suspected of violating provisions of the Act.

The Indian Telegraph (Amendment) Rules, of 2007, provided for lawful interception of telephone calls under [Rule 419A](#) with prior authorization by the Union or the State Home Secretary. It also provided for the validity of interception orders up to 60 days, extendable up to 180 days, and the assessment of the legality of the order by the Review committee.

Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, issued under Section 69 of the IT Act, allows the government and its agencies like IB, RAW, ED, NIA, CBI, and state police to intercept, monitor, or decrypt any digital communication with the approval of the competent authority. These [rules](#) were adopted alongside the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules in 2009. This latter was issued under Section 69B of the IT Act which allows government agencies to monitor traffic data for cybersecurity and national security reasons with the approval from the Union Secretary. It permits the reading of traffic patterns only and not the message content. In 2011, these were complemented by [Information Technology \(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information\) Rules](#) - these rules issued under Section 43A of the IT Act Define “Sensitive Personal Data or Information (SPDI)”, including financial, biometric, and medical records. They make it mandatory for companies and intermediaries to adopt reasonable security practices and require explicit user consent for data collection and sharing.

The [2016 Aadhaar \(Authentication\) Regulations](#), govern how the Unique Identification Authority of India (UIDAI) and requesting entities can perform and request authentication using the Aadhaar number. These regulations define methods like demographic, OTP, and biometric authentication, establish procedures for obtaining the Aadhaar number holder's consent, and outline the requirements for information sharing and the use of data to ensure privacy and security.

In 2021, the [Information Technology \(Intermediary Guidelines and Digital Media Ethics Code\) Rules](#) were adopted to impose the requirements for content moderation and data sharing as they require Significant social media intermediaries like What's App, Facebook, and Instagram to enable the traceability of the first originator of the messages, removal of content within 36 hours of the government order, and the appointment of compliance officers in India. It also brought digital news and OTT platforms under government surveillance.

[India's Digital Personal Data Protection Act, 2023](#), represents a significant step toward regulating personal data in the digital age, but it also raises concerns about state surveillance. While the law establishes a framework for processing personal data based on consent, transparency, and accountability, it grants sweeping exemptions to government agencies. Under Section 17, the state is permitted to process [personal data](#) without consent for reasons tied to national security, public order, and crime prevention, effectively allowing surveillance activities with minimal oversight. These broad allowances, coupled with the absence of an independent data protection authority with full autonomy, have sparked debate about the balance between individual privacy and state interests. Critics [argue](#) that while the Act aligns with global standards in some respects, its surveillance provisions risk undermining the fundamental right to privacy recognized by India's Supreme Court in 2017.

Case Law

Indian jurisprudence on digital surveillance has gradually evolved from a focus on legality and procedural safeguards to a more demanding standard of proportionality. The Supreme Court's landmark ruling in

PUCL v. Union of India (1996) introduced binding procedural guardrails, requiring authorisation by senior officials, reasons to be recorded, limited durations, periodic review, and eventual destruction of records. *K.S. Puttaswamy v. Union of India* (2017) elevated privacy to a fundamental right and required that all intrusions meet the tests of legality, necessity, and proportionality, including the use of the least-intrusive means. Subsequent cases tightened specific practices: *Anuradha Bhasin v. Union of India* (2020) curtailed indefinite internet shutdowns, insisting that orders be published, periodically reviewed, and time-bound, which pushed the government to reformulate suspension rules under the Telecommunications Act, 2023. High Court cases such as *Vinit Kumar v. CBI* (2019) and *Jatinder Pal Singh v. CBI* (2022) reinforced that interceptions without PUCL-mandated safeguards are unlawful, quashing or excluding such evidence. Meanwhile, the 2021 IT Rules' "traceability" mandate and the 2022 CERT-In logging and data-retention directions moved surveillance obligations upstream to platforms and infrastructure, sparking ongoing constitutional challenges around encryption and privacy. Finally, a statutory reform is underway, with the Telecommunications Act, 2023 replacing colonial-era powers, and new rules issued in 2024 to regulate shutdowns and pending draft interception rules seeking to embed PUCL-style safeguards in this modernised framework.

- *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 — Supreme Court (Dec 18, 1996)
Parties: PUCL (petitioner) v. Union of India.
What the Court held: [Telephone-tapping invades privacy](#); upheld s.5(2) but laid down binding safeguards (competent authority approval; limited duration; reasons recorded; periodic review; logs; destruction). These became the template for Rule 419-A (2007).
- *K.L.D. Nagasree v. Union of India*, Andhra High Court (Dec 11, 2006)
What the Court held: [Reiterated PUCL safeguards](#); found non-compliance with Rule 419-A procedures fatal to the interception. Shows High Courts enforcing the PUCL framework pre- and post-2007 insertion of Rule 419-A.
- *K.S. Puttaswamy (Retd.) v. Union of India* (Right to Privacy), (2017) 10 SCC 1 — Supreme Court (9J bench) (Aug 24, 2017)
What the Court held: [Privacy is a fundamental right under Articles 14/19/21](#); any surveillance must satisfy legality, necessity, and proportionality and have procedural safeguards, raising the bar for interception programs.
- [K.S. Puttaswamy \(Aadhaar\) v. Union of India, \(2019\) 1 SCC 1 — Supreme Court \(Sept 26, 2018\)](#)
What the Court held: Upheld core Aadhaar scheme for subsidies but struck down s.57 (private use) and read down disclosure provisions (e.g., s.33(2) national-security disclosure needed stronger oversight). The majority tied any identity-linked surveillance to strict statutory purpose and safeguards.
- [Vinit Kumar v. CBI, 2019 SCC OnLine Bom 3155 — Bombay High Court \(Nov 22, 2019\)](#)
What the Court held: Quashed three interception orders for lack of "public emergency/public safety" and absence of recorded reasons; ordered exclusion of the intercepted calls from evidence. Underscored that PUCL standards are

jurisdictional, not optional. (A later stay is noted in some materials; still widely cited on standards.)

- Jatinder [Pal Singh v. CBI, 2022 SCC OnLine Del 57 — Delhi High Court](#) (Jan 17, 2022)
What the Court held: Illegally intercepted calls are inadmissible; using such material would be “manifestly arbitrary” and violate fundamental rights. Re-affirmed that Rule 419-A compliance and PUCL standards are mandatory.
- Manohar Lal Sharma v. Union of India (Pegasus) — Supreme Court (Order, Oct 27, 2021; subsequent proceedings 2022–25)

What the Court held: [Court refused a “national-security” blank cheque](#), appointed an independent technical committee overseen by Justice R.V. Raveendran to probe alleged Pegasus use; later recorded committee findings (malware on some phones; no conclusive Pegasus confirmation) and continued monitoring, while declining blanket disclosure citing security. The Court asserted judicial review applies even where national security is invoked and insisted on fact-finding.

- WhatsApp LLC & Facebook v. Union of India (Traceability challenge) — Delhi High Court (filed May 2021; hearings through 2024–25)
Issue: [Rule 4\(2\)](#) of the 2021 IT Rules (first-originator traceability) allegedly breaks end-to-end encryption and violates privacy/free speech and proportionality. Government defends it as a narrow, order-based obligation grounded in s.69/s.87 of IT Act. *Status:* Pending; multiple hearings listed in 2024–25. This case will shape the legality of message-level “traceability.”
- Aakash Deep Chouhan v. CBI & Anr., CRL.M.C. 204/2020 — Delhi High Court (June 26, 2025)
What the Court held: Interception to tackle large-scale corruption can satisfy “public safety” under the (then-applicable) Telegraph s.5(2), if [PUCL/Rule-419-A](#) safeguards are met; the court declined to discard the tapped calls. This decision expands the scope of “public safety” beyond violence/terrorism when corruption threatens economic/public order interests. (Useful indicator for how “public safety” is being read post-Puttaswamy.)

2. PAKISTAN

Summary

Legal Framework

Pakistan’s Constitution (Article 14) guarantees the privacy and dignity of the home, and courts have affirmed that this extends to communications. In practice, however, several laws provide broad surveillance powers with limited oversight. The Pakistan Telegraph Act, 1885 (Section 5) - a remnant of British rule - permits the government to intercept messages on the occurrence of a public emergency or

for public safety. Modern statutes have added layers to the surveillance framework. The Investigation for Fair Trial Act, 2013 requires a judicial warrant for intercepting email, phone, or electronic communications in terrorism and other specified cases, theoretically ensuring prior court approval. The Prevention of Electronic Crimes Act, 2016 (PECA), a cybercrime law, enables real-time collection of data with a court's permission and obliges telecom providers to assist authorities, effectively facilitating state surveillance of online activities. Additionally, telecom license conditions and PTA (Pakistan Telecommunication Authority) regulations (2010 Monitoring Rules) require operators to install equipment for traffic monitoring and have even restricted encryption tools like VPNs without registration. Pakistan has no general data protection law in force yet, though a draft Personal Data Protection Bill, modelled on GDPR, is under consideration. This means intelligence agencies remain unchecked by any privacy regulator. A notable recent development is the establishment of a National Cyber Crime Investigation Agency (NCCIA) in 2024 under PECA to centralize digital investigations. Overall, Pakistan's legal regime allows extensive surveillance in the name of national security and public order, but vague definitions ("public safety," etc.) and weak oversight mechanisms (executive-controlled warrants and secret deployments) have created significant gaps. These gaps are evident in practices like the nationwide Lawful Interception Management System (LIMS) installed covertly to enable bulk monitoring of telecommunications, which had no clear statutory basis, illustrating how lawful authority is often outpaced by operational surveillance on the ground.

Case Law

Pakistan's higher judiciary has acknowledged the tension between state surveillance and individual rights, developing some checks. In a 1996 case brought by former Prime Minister Benazir Bhutto, the Supreme Court famously declared that blanket phone tapping and eavesdropping are illegal, immoral and unconstitutional, affirming that privacy extends beyond one's home into all spaces of life. The Court held that unauthorized surveillance violates fundamental rights (Article 14 on dignity/privacy and Article 19 on freedom of expression), a principle that invalidated the then-rampant tapping of politicians' calls. Subsequent rulings reinforced this stance. For example, in 2014 the Islamabad High Court struck down interceptions carried out without a court warrant, finding them in breach of the constitutional right to privacy. More recently, Pakistan's judiciary directly confronted the secret mass surveillance apparatus. In 2024, during a case about leaked phone conversations of public figures, the Islamabad High Court uncovered that the PTA had compelled telecom operators to install a "Lawful Intercept" system enabling agencies to access all mobile communications in real time. Justice Babar Sattar ruled that this unfettered surveillance violated citizens' privacy and due process, even suggesting officials involved could face criminal liability. He ordered telecom companies to bar any agency access absent lawful authorization. However, when the government appealed, the Supreme Court in August 2024 stayed the High Court's orders on procedural grounds, arguing the judge exceeded his jurisdiction. The final result is a mixed picture, since courts have rhetorically condemned unlawful spying and suppressed specific abuses, yet systemic reform has lagged. No Pakistani court has yet squarely ruled on spyware deployments (e.g. the use of Pegasus malware alleged by activists), and the Supreme Court's intervention to pause the LIMS judgment shows the judiciary's own limits in curbing the security establishment. Enforcement of [judicial guidelines](#) also remains inconsistent, but the case law at least establishes that any surveillance must be grounded in law and respectful of constitutional privacy, condemning unchecked fishing expeditions by the state.

2.1 Deployment

2013–2014: FinFisher Spyware Use Uncovered

In April 2013, cybersecurity researchers at Citizen Lab revealed the existence of [FinFisher](#) spyware servers operating inside Pakistan. Following this discovery, the NGO Bytes For All filed a petition in the Lahore High Court, prompting the court to order the Pakistan Telecommunication Authority (PTA) to investigate within 30 days. However, as of 2014 the PTA had failed to produce its report and the case stalled. Citizen Lab's technical evidence showed that FinFisher's command-and-control infrastructure was present on [Pakistani networks](#), strongly suggesting its use for covert monitoring.

By 2014, further leaks confirmed that someone in Pakistan had purchased [FinFisher](#) as early as 2010. An investigation by Digital Rights Foundation Pakistan (DRF) into a 40GB leak of FinFisher's internal data revealed a Pakistani client (identified as "Customer 32") who licensed multiple FinFisher tools for three years. The leaked FinFisher records show that FinSpy and FinUSB spyware were purchased by this Pakistani customer in April 2010, and a FinIntrusion Kit was added in June 2010. In total, the client spent roughly €300,000 on the FinFisher tool. Chat logs from FinFisher's support portal even indicate the user (alias "Khalid") sought advice on infecting targets via malicious PowerPoint files. DRF researchers note that no specific targets were named in the leak, but the scope and cost of the spyware suggest it was [deployed by Pakistani intelligence](#). Privacy advocates warned that such technology poses "serious threats" to journalists, human rights defenders, and activists in Pakistan, especially in the absence of privacy protections or oversight. [Despite](#) these findings and the ongoing court case, Pakistani authorities did not publicly reveal who was spied upon or which agency was behind FinFisher's use in Pakistan.

2015: Hacking Team leak and surveillance ambitions

In July 2015, a major breach of the Italian spyware company Hacking Team exposed extensive correspondence with clients worldwide, including over 1,000 emails involving actors claiming to represent Pakistani agencies. Hacking Team's flagship product at the time, the Remote-Control System (RCS), is malware that enables full remote takeover of computers and smartphones (similar in capabilities to FinFisher). The leaked emails (spanning 2011 through 2015) show Pakistani contractors negotiating to acquire RCS for top law enforcement and intelligence institutions. For example, early exchanges in 2011 involve a middleman claiming to represent the National Police Bureau and arranging demos of RCS for Pakistani officials at a Dubai security conference. By 2015, local representatives were still in talks with [Hacking Team](#), even requesting surveillance tools that could integrate with drones and land vehicles.

These communications reinforce that elements in Pakistan were actively seeking intrusive spyware like RCS. Privacy International's analysis of the leaks concluded that Pakistani companies attempted to procure Hacking Team malware on behalf of domestic law enforcement or intelligence clients in 2015. It remains unclear if a final deal was struck or if RCS was ever deployed in Pakistan, as many email threads ended when conversations shifted to phone or in-person meetings. No specific surveillance operations from Hacking Team's tools have been confirmed publicly in Pakistan. Nonetheless, the 2015 leaks highlighted Pakistan's ongoing interest in advanced digital spying capabilities, coming just a year after FinFisher's use was exposed. At this point, civil society groups grew increasingly concerned that such

“lawful intercept” spyware was being obtained from multiple international sources without public accountability.

2016–2018: Targeted digital attacks on civil society

By the late 2010s, reports indicated that digital surveillance of journalists and activists in Pakistan was widespread, even aside from commercial spyware suites. In 2017, the Digital Rights Foundation published accounts from seven Pakistani female journalists who believed they were under electronic surveillance. These women described extensive harassment and suspicious monitoring of their communications, underscoring how [journalists had become targets](#) in the digital realm. While specific spyware was not named in those cases, the pattern of intimidation was clear. One journalist noted that “every time I open an email, I am now scared”, reflecting fears of malware or hacking attempts.

In 2018, Amnesty International conducted a four-month investigation that uncovered a targeted hacking campaign against Pakistani human rights defenders. Attackers used fake online personas on social media to gain the trust of activists and then sent malicious links and files designed to infect victims’ devices with spyware. One prominent case was that of Diep Saeeda, a well-known civil society activist. After a fellow activist friend was forcibly disappeared in late 2017, Diep began campaigning for his release, and soon she herself was targeted. A Facebook account posing as an Afghan woman working at the UN contacted Diep, claiming to have information on her missing friend. The profile repeatedly sent her links to download files; these files contained mobile malware called “*StealthAgent*” that could spy on her smartphone if opened. The attackers also tricked her into revealing her email address, after which she received emails with a Windows spyware known as Crimson (a malicious program that would give attackers remote access to her computer). Diep grew suspicious and reported these attempts. Amnesty’s forensic analysis ultimately traced the malicious infrastructure and phishing pages back to a group of individuals based inside Pakistan.

Amnesty’s May 2018 [report](#), “Human Rights Under Surveillance: Digital Threats against HRDs in Pakistan,” confirmed that multiple activists had been targeted with spyware in similar ways. The campaign appeared aimed at surveilling and intimidating critics of the state, at a time when Pakistani civil society was already under severe pressure. These findings marked the first fully documented cases of local spyware operations against Pakistani activists, with Diep Saeeda and others singled out by name. It raised an alarm that not only were foreign-made tools being imported, but domestic actors were also developing or deploying spyware for political ends. Pakistani authorities did not announce any investigation into the [Amnesty findings](#); meanwhile, rights groups warned that such digital attacks, alongside threats and physical violence, were contributing to a climate of fear for journalists, bloggers, and peaceful dissenters.

2019: Pegasus spyware hits Pakistani officials

In mid-2019, [Pakistan](#) found itself on the receiving end of [surveillance](#) by NSO Group’s Pegasus spyware. In October 2019, WhatsApp and Citizen Lab revealed that Pegasus had exploited a vulnerability in WhatsApp to infect phones globally, sparking a lawsuit against NSO for abusing the platform. Among the 1,400 users attacked during that campaign, at least two dozen Pakistani officials’ phones were targeted and potentially compromised. According to sources cited by [The Guardian](#), the mobile devices of “scores of senior Pakistani defence and intelligence officials” were likely breached in this espionage operation.

The Pakistani government quietly investigated the incident, and reports suggest it suspected a foreign government was behind the surveillance. (Indeed, analysts pointed to India as the likely Pegasus operator in this case, given the ongoing rivalry and the parallel discovery of Pegasus being used against Indian activists and journalists around the same time). Although specific names of the Pakistani victims were not disclosed publicly, the breach was serious enough that Islamabad officials raised the issue. By December 2019, Pakistan's government expressed deep concern that such "state-on-state espionage" had occurred via Pegasus. In the aftermath, [Prime Minister Imran Khan's](#) team announced plans to develop a secure, Pakistan-made messaging app for government communications, seeking to reduce reliance on WhatsApp. The Pegasus incident of 2019 underscored that Pakistani authorities and even high-ranking officials were vulnerable to digital surveillance by external actors. It also highlighted how readily these commercial spyware tools could be turned against sovereign states, as well as domestic journalists, activists and dissidents.

2021: The Pegasus Project revelations

The issue of Pegasus spyware returned to the spotlight in 2021 with the Pegasus Project investigative series by media and human rights organizations. In July 2021, the leaked list of over 50,000 phone numbers selected for Pegasus targeting since 2016 was made public and included hundreds of Pakistani numbers. Among them was a phone number once used by Prime Minister Imran Khan, which had been marked as a possible target by an NSO client government. While the leaked records did not prove the phone was actually infected, the presence of his contact on the list raised alarm in Islamabad. The Pakistani government immediately said it would probe whether Khan's device had been hacked and promised to raise the issue in international forums.

According to The Washington Post (part of the Pegasus Project consortium), India was identified as one of the NSO client governments likely responsible for the Pakistani listings, including Imran Khan's number (India was among 10 countries flagged for extensive Pegasus use against civil society and officials). In reaction, Pakistan's Foreign Ministry condemned what it called "state-sponsored surveillance" by India and in a July 2021 statement it [urged the UN](#) to investigate India's abuse of spyware against Pakistani public figures. Beyond the prime minister, the leaked data suggested that numerous other Pakistanis, including opposition politicians, diplomats, journalists and activists, had been selected as targets, although their identities have not been fully disclosed. No evidence emerged that Pakistan's own agencies were Pegasus clients, and Pakistan was not named among the countries believed to use NSO spyware. Nevertheless, the Pegasus Project revelations illustrated how journalists and civil society in Pakistan can become surveillance targets amid regional political espionage. Pakistani ministers decried the "unethical policies" behind such spyware abuse and joined international calls for greater regulation of the global surveillance industry.

2.2 Legal Framework

Norms

Article 14 of the Pakistan Constitution establishes a [fundamental right to privacy](#), not only within the home but also in public and digital spaces, as affirmed by Supreme Court rulings. For instance, a landmark ruling in 1996 invalidated unauthorized phone tapping as a violation of privacy and free expression. Article 19 protects [freedom of speech](#).

Some [legislation](#) from the Colonial-era is still in force and could apply to digital surveillance. In particular, the [Official Secrets Act \(1923\)](#) remains active, criminalizing unauthorized disclosure or possession of “official secrets” and [permitting searches and seizures](#) to protect national security. This older law underpins modern surveillance justifications in [sensitive contexts](#). The Telegraphs Act of 1885 (Section 5) allows [interception of communications](#) in the event of a “public emergency” or in the name of public safety, based on a government-issued certificate.

More recent legislation, such as the [Investigation for Fair Trial Act \(IFTA\)](#), adopted in 2013, permits interception of data (such as emails, calls, or computer communications) through a judicial warrant, based on “reasonable belief” of criminal planning or association. Surveillance under this act is limited to 60 days, though no warrant appears to have ever been issued in its initial 11 years of existence.

The 2016 Prevention of Electronic Crimes Act (PECA) is Pakistan’s primary legislation targeting cybercrime, including cyberstalking, online harassment, forgery, blasphemy, and cyberterrorism. While focused on crime, it also enables state surveillance and data access as part of its enforcement tools.

Although Pakistan has not yet enacted a comprehensive data protection law, drafts have been in development. [The Personal Data Protection Bill \(PDPB\) 2023](#) is modelled on the EU's GDPR and introduces consent-based processing, purpose limitation, data localization, and more. The National Commission for Personal Data Protection (NCPDP) has been established under the [draft bill](#) to adjudicate complaints, enforce rules, and impose substantial fines.

In May 2024, the National [Cyber Crime Investigation Agency \(NCCIA\)](#) was established (under Section 51 of PECA) as a specialized successor to the Federal Investigation Agency’s cybercrime wing. It handles [PECA enforcement and cybercrime investigations](#). The agency has already conducted significant [actions](#), such as arrests related to massive online fraud and IMEI tampering in mid-2025.

In January 2025, Parliament amended PECA to introduce a Social Media Regulatory Authority, backed by its own investigative agency and tribunals empowered to impose prison sentences up to three years and fines up to PKR 2 million for alleged “fake or false” content. Journalists and rights groups widely [condemned](#) the move.

The government’s recent move toward VPN registration and licensing, coupled with ideological backing from religious authorities, signals an [attempt to control](#) secure communications and curb surveillance evasion.

Case Law

In the 1990’s, the Supreme Court held surveillance to be unlawful, immoral, and unconstitutional in the [case](#) of *Mohtarma Benazir Bhutto & Others vs. President of Pakistan and Ors.* [Privacy](#) extends beyond one’s home into public spaces, and any illegal intrusion violates human dignity and constitutionally guaranteed rights, including life and freedom of expression (Articles 14, 19).

In 2014, in the *Pakistan Telecom Mobile Ltd. vs. Federation of Pakistan* case, [courts](#) ruled on the legality of intercepting calls without a valid court order, holding that such interception violates the right to privacy. Three years later, in *Muhammad Akbar v. The State*, courts clarified that national security cannot serve as a blanket pretext to infringe individual rights.

In 2024, during a hearing at the Islamabad High Court (IHC) in a case brought by Bushra Bibi and Najam Saqib, it was revealed that the Pakistan Telecommunication Authority (PTA) had mandated telecom companies to [“finance, import, and install”](#) the Lawful Intercept Management System (LIMS) at designated “surveillance centres,” enabling state agencies mass access to telecom users’ data without oversight or explicit legal authorization. Through the use of LIMS, a designated agency can initiate a track-and-trace request (e.g., for a SIM, IMEI, or phone number). This request passes through LIMS (automated, no human review) into the telecom operator’s network. The [system](#) automatically provides access to SMS, call metadata, voice and video content, and browsing histories, which is then transmitted to a surveillance centre. The court ruled that since LIMS was installed unlawfully, agencies using it are liable for criminal actions. The IHC temporarily barred telecom companies from allowing LIMS access to their networks or consumer data. The court directed [PTA](#) to submit a sealed report detailing the procurement, installation, and access to LIMS. In August 2024 the Supreme Court stayed the IHC’s proceedings and orders, ruling the IHC had exceeded jurisdiction. The federal government had challenged that the IHC’s broad orders were beyond its scope. The Supreme Court issued notices and restrained further [IHC action](#).

3. KENYA

Summary

Legal Framework

Kenya’s 2010 Constitution provides a strong starting point for privacy. Article 31 guarantees every person the right to privacy, including the right not to have their communications infringed without lawful justification. Building on this, Kenya has enacted both general data protection legislation and sector-specific surveillance laws.

The Data Protection Act, 2019 created an independent Office of the Data Protection Commissioner (ODPC) to regulate personal data processing across public and private sectors. The DPA – together with its 2021 regulations – requires data controllers (even security agencies) to follow principles like data minimization and to conduct Data Protection Impact Assessments (DPIAs) for high-risk surveillance initiatives. In parallel, statutes targeted at national security anchor Kenya’s interception powers. The National Intelligence Service Act, 2012 permits the intelligence agency to undertake special surveillance operations with a High Court warrant, ensuring a judge’s approval for intercepting communications. Similarly, the Prevention of Terrorism Act, 2012 allows police to apply to court for interception orders in terrorism investigations.

These laws embed the constitutional principle that surveillance is only lawful if authorized by a court and necessary for specified serious crimes. For everyday law enforcement, the Computer Misuse and Cybercrimes Act 2018 criminalizes unauthorized access and interception, while empowering authorities (with warrants) to search and seize stored data or conduct real-time collection in cybercrime cases. In addition, Kenya’s Information and Communications Act (KICA) mandates telecom operators to uphold the confidentiality of communications and only disclose data if compelled under law. Recent SIM card registration regulations (2025) under KICA tighten ID verification and require telcos to retain subscriber

data, but also explicitly bind them to data protection obligations, a dual regime meant to facilitate law enforcement access while guarding against misuse.

In practice, however, compliance and oversight remain challenges. Civil society has flagged instances of agencies attempting to bypass proper procedure. For example, a controversial plan to install a Device Management System on mobile networks was initially pursued without public participation or adequate privacy safeguards. Kenya does have institutional checks: the judiciary (through warrants and evidence rules), the ODPC (handling privacy complaints), and the Communications Authority (ensuring telecommunications companies cooperate lawfully). Together, Kenya's framework is regarded as comparatively robust on paper, balancing security needs with privacy rights, though its true test lies in enforcement and resisting pressures to conduct blanket surveillance in the name of security.

Case Law

Kenyan courts have actively shaped the contours of digital surveillance, often invoking constitutional principles. In *Coalition for Reform and Democracy (CORD) v. Republic of Kenya* (2015), which reviewed new security laws, the High Court upheld provisions allowing intercepts for intelligence and counterterrorism, finding that requiring a High Court warrant under the NIS Act and PTA was constitutionally sufficient and did not infringe Article 31 privacy protection. However, courts have been quick to strike down surveillance measures lacking legal footing. A notable example was the "Device Management System" (DMS) dispute: in 2018, the High Court (in *Okiya Omtatah Okiiti v. Communications Authority*) stopped the telecom regulator from installing tapping equipment on mobile networks, citing privacy violations and a lack of public consultation. Judges ruled that connecting a system to monitor all mobile devices posed an unconstitutional threat to privacy. Although the Court of Appeal later reversed that blanket injunction (deciding in 2020 that the DMS could proceed if proper safeguards and stakeholder consultations were implemented) this was framed as a procedural adjustment rather than a repudiation of privacy concerns. The case led to Kenya's Supreme Court ultimately granting permission in 2023 for a limited DMS rollout, even as digital rights groups warned of mass surveillance risks.

Beyond interception, Kenyan courts have enforced privacy-by-design in governance initiatives. In *Nubian Rights Forum v. Attorney General* (2020), the High Court allowed Kenya's new biometric ID system (Huduma Namba) to proceed only under strict conditions – that there is no collection of DNA/GPS data and full implementation of the Data Protection Act first. The Court underscored that absent a comprehensive data protection framework, such a mass system would violate privacy, effectively stalling the project until safeguards were in place. Furthermore, when the government later rolled out Huduma ID cards without conducting a DPIA, the High Court in 2021 (in *Katiba Institute v. Mucheru*) suppressed the rollout for breaching the Data Protection Act's requirements. Courts have also dealt with day-to-day surveillance scenarios. For example, illegally obtained phone evidence has been deemed inadmissible (e.g. the 2019 *Blogger's* case upheld the Cybercrimes Act's investigatory powers but implied that any digital search must have judicial authorization). Even private surveillance has come under scrutiny. In 2023, a court in *Ondieki v. Maeda* held that a neighbour's CCTV pointing at someone else's property violated the constitutional right to privacy and ordered it re-angled. Through these cases, Kenyan jurisprudence has accepted targeted surveillance that is lawful and warranted, but is increasingly intolerant of dragnet or extra-legal monitoring. The courts have demanded public transparency, proportionality, and adherence to data protection standards (like DPIAs) before intrusive technologies are deployed.

3.1 Deployment

Early 2010s: Laying the groundwork for surveillance

In the early 2010s, Kenyan authorities began significantly expanding their intelligence apparatus and technical surveillance capabilities. By 2012, the number of personnel [“paid to spy” on citizens and perceived enemies of the state](#) had swelled by an extra 1,500 ahead of the 2013 elections. Around the same time, reports emerged of new electronic surveillance tools entering use. A Blue Coat PacketShaper device, capable of deep packet inspection and filtering of internet traffic, was detected on Kenyan networks in January 2013, raising concerns that the government could monitor or censor online communications under the guise of countering “inflammatory” content.

Also in this period, Kenyan security agencies obtained equipment for intercepting mobile phone traffic. The National Intelligence Service (NIS) was reportedly the first to acquire an IMSI catcher (a device that masquerades as a cell tower to intercept calls and texts) as far back as 2007. By the early 2010s, at least two covert [IMSI catcher units were in operation](#), one controlled by NIS (stored at its Nairobi headquarters when not deployed) and another used by Kenyan police investigators. These early deployments laid a foundation for more advanced digital surveillance in subsequent years.

The Westgate Mall terrorist attack of September 2013 marked a turning point that accelerated Kenya’s investment in surveillance technology. In the wake of the attack, which killed 67 people, the government embarked on an aggressive “overhaul of its surveillance regime” as part of re-examining national security policies.

Surveillance capabilities were seen as critical to preventing further terror incidents. Notably, in 2014 the government turned to Chinese telecom giant Huawei to build Africa’s first “Safe City” system in Nairobi. Under a joint contract with Kenya’s leading telecom operator Safaricom, an Integrated Urban Surveillance System was launched, deploying hundreds of networked CCTV cameras across Nairobi’s streets and highways. By 2015 the city had nearly 2,000 high-definition cameras feeding into a new police command centre. This modern digital CCTV network (Huawei’s pilot [Safe City project](#) on the continent) put real-time surveillance tools into the hands of thousands of police officers for the first time. These early 2010s initiatives underscore how Kenya began blending human intelligence with emerging digital surveillance, setting the stage for more covert and sophisticated programs to come.

Mid-2010s: Adopting advanced spyware and interception systems

By the mid-2010s, Kenya’s surveillance toolkit grew to include state-of-the-art spyware and interception platforms. In 2015, research by the University of Toronto’s [Citizen Lab](#) uncovered the presence of FinFisher spyware operating in Kenya. Citizen Lab’s scans identified a FinFisher command-and-control server on an IP range registered to “National Security Intelligence,” strongly indicating that Kenya’s NIS was running the spyware. This finding provided concrete evidence that Kenyan intelligence had acquired FinFisher malware to secretly monitor computers or phones, a tool known to have been abused elsewhere against journalists and dissidents. Contemporaneous [reporting](#) suggested that NIS had “purchased software to crack websites,” allegedly from FinFisher, as part of its expanding cyber surveillance capabilities.

Around the same time, Kenya was exploring trading with other foreign surveillance tech vendors. Leaked emails from the Italian company Hacking Team (after its own breach in 2015) revealed that Kenyan officials had negotiated to buy Hacking Team's Remote-Control System (RCS) spyware. In April-May 2015, NIS agents corresponded with Hacking Team seeking to procure RCS, and even went so far as to request a "proof of concept" attack on a [website](#) that had been critical of the government. Specifically, an NIS agent asked Hacking Team to demonstrate its hacking capabilities by taking down a popular corruption news blog *Kahawa Tungu* that was troublesome to Kenyan authorities. This unusual request laid bare the agency's intent to use digital surveillance tools directly against domestic journalists and critics of the regime. [Hacking Team](#) ultimately declined to fulfil the hack or complete the sale, reportedly due to concerns about Kenya's intended use of the spyware. Still, the episode highlighted the government's determination at the time to acquire intrusive surveillance malware for use against journalists, activists, and opposition voices at home.

Meanwhile, Kenya continued to invest in more routine telecom interception infrastructure. Lawful intercept probes and data collection systems were quietly [installed within telecom networks](#). Safaricom and other operators were required to accommodate government monitoring, often with minimal transparency. In 2014, Parliament had controversially amended security laws to broaden NIS powers, including the ability to monitor communications without a warrant, which facilitated the deployment of interception gear at ISP backbones and mobile switching centres. The practical effect was that by the mid-2010s Kenyan security agencies had gained direct access to communication flows. Privacy International investigators noted that NIS "appears to have direct access to communication networks across Kenya," allowing surveillance of phone calls and data with little need to involve the service providers. Sources suggested that some telecom engineers were kept in the dark, as interceptions occurred at network backdoors controlled by intelligence officials. This period also saw the roll-out of the Integrated Public Safety surveillance project (Safe City) in Nairobi and Mombasa, embedding always-on monitoring via cameras and integrated communications for law enforcement.

By 2015, Kenya had aggressively embraced an array of digital surveillance tools, from malware to monitoring centres, with an eye toward both fighting security threats and keeping tabs on government critics. These capabilities, largely acquired under the administration of President Uhuru Kenyatta (2013–2022), would soon be put to use in high-stakes political contexts.

Late 2010s: Widening the surveillance net

In the late 2010s, Kenya's digital surveillance expanded further, both in scope and sophistication. One controversial initiative was the government's attempt to implement a Device Management System (DMS) on mobile networks, which civil society warned would become a mass surveillance tool. The Communications Authority of Kenya introduced the [DMS in 2016 under the pretext of identifying counterfeit phones](#). Telecom companies and activists quickly sounded the alarm. In 2017, Safaricom and Telkom Kenya publicly refused to fully integrate the DMS, warning that it could grant the state access to customers' call records and messages without consent. The DMS hardware installed at mobile operators would theoretically absorb IMEI device identifiers, but it also raised the [possibility](#) of drawing off subscribers' personal data (location, call logs, SMS) in real time.

Safaricom's CEO at the time even acknowledged the "high probability that third parties may have access to calls and messages" if the system went live. In early 2018, Kenya's High Court halted the DMS, labelling it "a threat to the subscribers' privacy" and ordered regulators to pursue less intrusive

measures. This legal victory for privacy was short-lived; the government appealed, and higher courts later cleared DMS with some conditions. But it exemplified the ongoing dispute between Kenya's surveillance ambitions and privacy advocates. By 2019, the state was still intent on leveraging the DMS or similar systems, despite public outcry. In fact, as of 2023 the Supreme Court ultimately allowed DMS to proceed, sparking fresh concerns among digital rights groups.

At the same time, Kenya was reportedly procuring cutting-edge surveillance platforms from abroad. Investigative research in 2018–2020 revealed Kenya as a client of the Israeli company NSO Group and its affiliates. [Citizen Lab's 2018 global scan of NSO's Pegasus spyware](#) found evidence of Pegasus operators active inside Kenya. While specific targets in Kenya were not publicly named, the presence of a [Pegasus system](#) strongly implied that high-value individuals were in the crosshairs of state surveillance.

In late 2020 Citizen Lab identified Kenya as one of 25 countries using the Circles surveillance platform. Circles (an NSO Group affiliate) sells technology that exploits vulnerabilities in SS7 mobile signalling to intercept calls, texts, and track phones without requiring any malware on the device. Simply by entering a phone number, Circles clients can secretly obtain a user's call logs or live location via the telecom network's backbone. According to African Arguments, a Circles system was detected operating in Kenya, which observers saw as unsurprising given the Kenyatta government's aggressive stance against dissent. "In Kenya, freedom of expression and media freedoms are under constant threat... The government relies heavily on surveillance of its citizens to crack down on any form of opposition," noted one Nairobi-based researcher in 2021.

Indeed, throughout the late 2010s, opposition politicians and activists increasingly reported being monitored. There were instances of mysterious phone call leaks and surveillance of encrypted communications during contentious events like the 2017 elections and subsequent protests. While authorities claimed such capabilities were to fight terrorism and crime, the same tools were turned inward to quash political challenges. For example, domestic intelligence reportedly monitored the communications of opposition leader Raila Odinga's circles during the 2017 election period (as inferred from later media accounts and activists' testimonies), though much of this occurred covertly. [The Privacy International investigation Track, Capture, Kill \(2017\)](#) documented how intercepted communications were fed into "a cycle of arrests, torture, kill or disappear" in Kenya's counterterrorism operations, a pattern that human rights groups warned could easily be applied to silence regime critics.

By 2019, Kenya had built a formidable digital dragnet: spyware tools, telecom intercept systems (like Circles and IMSI catchers), and broad data access agreements with service providers, all used with minimal transparency.

2020s: Ongoing surveillance and exposés

In the 2020s, Kenya's use of digital surveillance has continued unabated, though it is increasingly coming to light through investigative reporting and whistleblowers. A watershed moment arrived in late 2024, when the Nation Media Group published a detailed exposé on the country's surveillance practices.

The Nation's investigation revealed that Safaricom, Kenya's largest telecom operator, had been routinely providing security agencies with direct access to customers' data without court orders. According to the report, Safaricom allowed police and intelligence units to retrieve subscribers' call records, geolocation pings, and other personal data in bulk, under informal arrangements purportedly for "security"

purposes. Such data handovers were done quietly and frequently, outside of any transparent legal process. The exposé linked these surveillance tactics to a pattern of abuses including enforced disappearances and extrajudicial killings of suspects. In some cases, individuals who were tracked via their mobile phone data later turned up dead or vanished, suggesting their real-time phone location was used to kidnap or eliminate them. Safaricom, notably, did not refute the substance of these allegations. Instead, the company attempted to deflect attention by attacking the messengers. In the weeks following the publication, Safaricom launched a punitive legal complaint against the Nation Media Group and its journalists, a move widely seen as a SLAPP (strategic lawsuit against public participation) aimed at silencing them. Safaricom accused the reporters of unethical conduct and even pressured Kenya's media regulator to sanction the outlet, despite the fact that the journalists had repeatedly sought the company's input before publishing.

Observers pointed out that Safaricom conspicuously failed to deny the core claims of collusion in unlawful surveillance. The Kenya Human Rights Commission and other NGOs condemned [Safaricom's reaction as an attempt "to evade scrutiny" of its role](#) in enabling state surveillance that endangers lives. The episode is telling, for it confirms through credible, published evidence that Kenyan authorities have access to telecom data on a wide scale, and that this access has been used to target individuals outside of legal channels.

International partners also took notice. In [October 2024](#), the U.S. Ambassador to Kenya publicly reprimanded Kenyan security agencies for unlawful mobile phone surveillance, calling it a breach of privacy and the rule of law. Her remarks came after *The Nation* exposé showed how police obtain private phone details with ease. The ambassador urged Kenyan authorities to respect privacy rights, underscoring that surveillance must follow due process. Safaricom, feeling the heat, issued statements insisting that it only shares data "when explicitly required via a court order," a claim met with scepticism given the mounting documented evidence to the contrary.

Digital rights advocates note that Kenya did finally enact a Data Protection Act (in 2019) and set up a data commissioner, but these have offered little practical restraint on security organs in practice. Unchecked surveillance has spilled into other arenas as well. During the #EndCOVIDLockdown and #RejectFinanceBill protests of 2020–2023, activists reported that police were tracking protest organizers through phone surveillance and social media monitoring. According to CIPESA, authorities deployed ["sophisticated digital tools to monitor protestors"](#) without oversight, alongside physical crackdowns. Encrypted messaging apps and VPN usage spiked among civil society groups in an attempt to evade government eavesdropping during sensitive campaigns.

As of 2025, Kenya's digital surveillance complex is at a crossroads. The past 10-15 years have seen the country acquire and employ an extensive range of spy technology, from malware implants (FinFisher, Pegasus) to telecom intercept systems (Circles' SS7 exploits, IMSI catchers), internet monitoring appliances (Blue Coat), and large-scale data analytics programs pulling from telecom and financial records. These tools have been used in high-profile counterterrorism efforts, but also against journalists, activists, opposition politicians, and even international investigators. Kenyan police and intelligence agencies have intercepted journalists' communications, spied on NGO workers, and shared surveillance data with allied regimes (for instance, there is evidence Kenyan services cooperated in monitoring or rendition of exiled Rwandan and South Sudanese dissidents via cell phone data). The culture of

surveillance that took root in the 2010s continues today, even as brave journalism shines light on its abuses.

The [Kenyan government](#) has consistently defended these programs as necessary for national security. Yet the documented cases, such as the Safaricom revelations of 2024, show how easily such surveillance is turned against civil society. Moving forward, Kenya faces growing calls to halt its surveillance practices. Without stronger oversight and transparency, digital surveillance will remain a powerful tool that can be (and has been) weaponized against the very citizens it purports to protect.

For now, the narrative of the past decade and a half is clear. Kenya's surveillance state has rapidly evolved, deploying cutting-edge spyware and monitoring systems, and its targets have often been those who speak truth to power – journalists uncovering corruption, activists mobilizing for justice, and opposition figures challenging authority. Each new disclosure and whistleblower account further illuminates the extensive reach of these programs, underscoring the urgent need for accountability in Kenya's digital surveillance regime.

Mary Wachuka Maina

- **Victim/Target:** In Kenya, the targets of spyware have included journalists, opposition figures, and even members of the president's own team. A prominent case emerged in 2024 when court filings by Mary Wachuka Maina – a Kenyan-Canadian software developer – revealed a [secret government surveillance project](#) aimed at media and political rivals. According to her lawsuit, the spyware project was intended to profile and monitor journalists, media houses, opposition leaders, and even manipulate social media trends ahead of the 2027 election. The software's design would allow searches on journalists and compilation of dossiers to undermine critical media reporting.
- **Spying Entity:** The alleged perpetrators were high-level aides in President William Ruto's administration, including his communications secretary and a top public service official, who was accused of orchestrating the plan. The lawsuit claims these officials, with the President's approval, contracted Maina to develop the surveillance system using state funds from a secret account. Essentially, elements within the Kenyan government (State House) were behind the scheme, intending to use it as a tool for political espionage and propaganda.
- **Technology Used:** The case revolved around a custom-built spyware platform (codenamed "Numera 2023"). Unlike off-the-shelf spyware, this was a bespoke digital surveillance and disinformation system. It was to incorporate mobile device hacking (covertly spying on targets' communications), social media control (hijacking accounts, deleting unfavourable comments), and data analytics for profiling ethnic sentiment and opposition activity. In essence, it was a comprehensive digital surveillance suite tailored for the Kenyan context.
- **Confirmation Methods:** The existence of the spyware project was confirmed through legal evidence in Maina's court filings. She provided contracts, meeting notes, and correspondence with officials detailing the tool's specifications (for example, the ability to infiltrate phones and monitor

journalists). This documentary evidence, now part of the public court record, was further bolstered by investigative journalism. Kenyan media (e.g. Nation Media Group) obtained copies of the court papers and broke the story, causing a public outcry. The corroborating evidence included proof of payment transfers and emails from officials instructing her to proceed with the spying project.

- **Actions Taken:** Mary Wachuka Maina took legal action by filing a lawsuit in Kenya's High Court in late 2024, suing four senior government officials and aides for breach of contract and exposing the clandestine surveillance plan. She sought compensation for her losses and, notably, a court order restraining the officials from threatening her after she started receiving "menacing death threats" over the dispute. Her bold step effectively blew the whistle on the operation. In response to the revelations, Kenyan civil society and opposition leaders launched campaigns demanding accountability. The scandal was debated in Parliament, and NGOs called for an independent investigation into the abuse of public funds for spying.
- **Outcomes/Responses:** The immediate result was a public controversy and greater scrutiny of government surveillance. President Ruto's spokespeople issued denials; the spyware project was halted before full deployment. The High Court case is ongoing. As a retaliation, [authorities](#) reportedly tried to intimidate Maina (even attempting to cancel her Kenyan passport). While no one has yet been penalized, the exposure itself forced the government to at least pause the program and prompted Kenya's data protection authority to announce it would audit government surveillance contracts. The case also stands as a rare example of an insider challenging a secret cyber-operation through the courts. Its progress is being watched by press freedom groups – if Maina prevails or if officials are compelled to testify, it could set a precedent for judicial oversight of digital surveillance in Kenya. At the very least, the scandal spurred public awareness and debate about unchecked surveillance, hopefully paving the way for stronger legal safeguards.

3.2 Legal Framework

Norms

At the highest level, [Kenya's 2010 Constitution](#) provides the foundational safeguard for digital privacy and surveillance. Article 31 guarantees every person the right not to have their person, home, or property searched or their private communications infringed without lawful justification. This means all subsequent legislation on interception, data collection, or monitoring must be read in light of a constitutional baseline, that is, surveillance powers must be clearly established by law, reasonable, and justifiable in an open and democratic society. Article 31 is the standard through which the proportionality and legality of surveillance measures are assessed by courts.

The [Data Protection Act, 2019 \(DPA\)](#) builds on that constitutional guarantee by setting out a horizontal regulatory framework. It introduces the Office of the Data Protection Commissioner (ODPC) as an

independent regulator empowered to register data controllers and processors, investigate complaints, issue penalty notices, and enforce compliance. The DPA applies to both private companies (such as telecom operators, internet platforms, and financial services) and public bodies, including security and intelligence agencies, when they process personal data. The [2021 Regulations under the Act](#) give teeth to this framework:

- The General Regulations codify privacy by design/default and require Data Protection Impact Assessments (DPIAs) for high-risk activities like systematic monitoring or large-scale processing
- [The Complaints and Enforcement Regulations](#) provide a structured path for citizens to challenge intrusive practices
- [The Registration Regulations](#) impose a transparency obligation on entities engaged in sensitive or large-scale processing.

Thus, before intelligence or police bodies can even process communications data, they are formally subject to DPA standards, unless exempted under national security grounds, a point that has already generated debate within Kenya's courts and civil society.

Targeted surveillance for national security or counter-terrorism purposes is enabled by security-specific statutes. The [National Intelligence Service Act, 2012](#) allows the Service to undertake "special operations" such as monitoring or intercepting communications, but only with a High Court warrant. This embeds a judicial authorization mechanism directly into the statute, reflecting constitutional safeguards. The Act also established the Intelligence Service Complaints Board, offering a path of recourse for abuses. Similarly, the [Prevention of Terrorism Act, 2012 \(PTA\)](#) empowers authorities to apply for interception orders to prevent or investigate terrorist acts, also requiring judicial authorization. These laws show a clear design, allowing surveillance but tied to warrants and judicial oversight, at least on paper, though civil society has raised concerns about compliance and secrecy in practice.

For digital crime and broader state access to computer data, [the Computer Misuse and Cybercrimes Act, 2018 \(CMCA\)](#) provides a dual track. It criminalizes unauthorized interception (making illegal surveillance punishable), while at the same time enabling law enforcement to conduct lawful access under judicial warrants. Specific provisions allow for search and seizure of stored computer data, real-time collection of traffic data, and interception of content, including via mutual legal assistance (MLA) with foreign states.

In practice, this means Kenyan authorities cannot lawfully demand "live" internet traffic or stored digital evidence from a service provider without following the procedural safeguards embedded in the CMCA. The [2024 Critical Information Infrastructure and Cybercrime Management Regulations](#) operationalize these duties further, requiring entities designated as "critical information infrastructure" (such as telecoms or financial networks) to implement cybersecurity measures, reporting obligations, and audits. These regulations create a compliance backbone through which the state both receives incident information and can leverage points of access to data.

[The Kenya Information and Communications Act \(KICA\)](#) remains the central telecom statute. Section 31 of KICA requires licensed operators to preserve confidentiality of communications and prohibits interception or disclosure except as authorized by law. This aligns KICA with the Constitution's privacy guarantee, effectively making it unlawful for telcos to cooperate with surveillance without a lawful order.

The operational link comes via the [Registration of Telecommunications Service Subscribers Regulations, 2025](#), which replaced the earlier 2015 SIM-card rules.

These new rules tighten identity verification, requiring operators to validate subscriber information against government databases and prohibiting proxies (except for children and dependents). They also oblige operators to retain subscriber data, share periodic compliance reports with the Communications Authority, and deactivate unverified SIMs. Crucially, they expressly impose data-protection obligations on telecoms, which means that surveillance through SIM registration or subscriber databases must comply with both KICA and the DPA. This creates a dual compliance duty, since operators are legally required to hold accurate subscriber data for regulatory purposes, but also required to protect that same data against misuse or unauthorized surveillance.

Sectoral rules fill in additional gaps. [The Civil Aviation \(Unmanned Aircraft Systems\) Regulations, 2020](#) regulate the operation of drones, indirectly controlling forms of aerial surveillance. The regulations require drone operators to hold valid licenses, restrict flights over sensitive areas, and enforce privacy obligations in line with the DPA. Similarly, when law enforcement or intelligence services use drone surveillance, the DPA and constitutional privacy provisions still apply, ensuring a balancing test between security aims and privacy rights. On the back end, when digital surveillance evidence reaches court, [the Evidence Act \(Cap. 80\)](#) governs admissibility of electronic records under sections 106A and 106B. Courts have consistently demanded proper certification and authentication of electronic evidence, which means that even surveillance-derived material must clear evidentiary hurdles before being used in prosecutions.

Institutionally, this framework is policed by three key actors: the ODPC as the privacy and data-protection regulator; the Communications Authority (CA) as the telecom regulator overseeing subscriber registration and operator compliance; and the Judiciary, which authorizes surveillance through warrants (under the NIS Act, PTA, and CMCA) and decides on admissibility of surveillance-derived evidence under the Evidence Act. Together, these authorities form an overlapping system of ex-ante control (warrants, registration, compliance) and ex-post accountability (ODPC enforcement, complaints, judicial remedies).

The CMCA's MLA provisions allow foreign states to request Kenyan authorities to intercept traffic data or content in real time, provided proper legal channels and judicial authorizations are followed. This positions Kenya within international cybercrime and surveillance cooperation frameworks, while still tethering access to domestic constitutional safeguards and statutory procedures.

Case Law

Kenyan courts have been building a body of surveillance-relevant jurisprudence for a decade. In [Coalition for Reform and Democracy \(CORD\) & 2 others v Republic of Kenya & 10 others \(2015\)](#), a three-judge bench reviewed challenges to the Security Laws (Amendment) Act and, while striking out several provisions on speech and criminal process, upheld surveillance-adjacent powers, holding that the then new s.42 of the National Intelligence Service Act and s.36A of the Prevention of Terrorism Act were constitutional and did not violate Article 31 privacy, signalling early judicial acceptance of targeted interception under warrant and within statutory limits.

Later that year, in [*Bernard Murage v Fineserve Africa Ltd & 3 others*](#), the High Court was asked to halt roll-out of “Thin-SIM” technology over fears of data interception; the Court confirmed that threatened violations of privacy can ground a constitutional petition but declined relief for lack of concrete proof and emphasized it could not compel Parliament to enact a data protection law, an early articulation of evidentiary thresholds and institutional roles in privacy litigation. In 2018, two consolidated “Device Management System (DMS)” cases challenged the regulator’s plan to plug equipment into mobile networks. [*Okiya Omtatah Okiiti v Communications Authority of Kenya & 8 others \(High Court, 19 Apr 2018\)*](#) found the DMS rollout unlawful for lack of public participation and for posing a threat to privacy, and [*Kenya Human Rights Commission v Communications Authority of Kenya & 5 others*](#) the same day likewise faulted the DMS for procedural and privacy defects. Both decisions leaned heavily on constitutional due-process duties around surveillance capabilities. On appeal, however, the Court of Appeal in [*Communications Authority of Kenya v Okiya Omtatah Okiiti & 8 others \(24 Apr 2020\)*](#) set aside the blanket invalidation, holding the project was still at a design stage and ordering the Authority to continue technical work subject to consultations and public participation, thus reframing the dispute from a per se privacy violation to one of procedural safeguards and governance over powerful monitoring tools.

Also in 2020, the High Court’s landmark NIIMS/Huduma Namba judgment - [*Nubian Rights Forum & others v Attorney General & others \(30 Jan 2020\)*](#) - allowed Kenya’s single-registry biometric ID to proceed only under strict conditions, including a comprehensive legal and regulatory framework compliant with the (new) Data Protection Act - no collection of DNA or GPS coordinates, and heightened safeguards before data integration and sharing - thereby importing proportionality and data-minimisation principles into population-scale identity systems.

In [*Bloggers Association of Kenya \(BAKE\) v Attorney General & others \(20 Feb 2020\)*](#), the Court largely upheld the Computer Misuse and Cybercrimes Act, including investigative powers that can facilitate digital searches and data access under judicial oversight, while curbing a few speech-related offences, which constituted an important confirmation that cybercrime tools are constitutional so long as warranted and proportionate. As implementation moved forward, the *High Court in* [*Republic v Joe Mucheru, CS ICT & others; Katiba Institute & Yash Pal Ghai \(ex parte\) \(14 Oct 2021\)*](#) quashed the Huduma Card rollout for failure to conduct a [*Data Protection Impact Assessment \(DPIA\)*](#) and for inadequate public participation, insisting that mass-ID schemes meet Data Protection Act duties before deployment.

Courts have also begun shaping everyday digital watching via CCTV. In [*Ondieki v Maeda \(31 May 2023\)*](#) the High Court held that home CCTV aimed beyond the owner’s premises can breach Article 31 privacy and ordered less intrusive positioning, warning that ubiquitous cameras must be justified, necessary and proportionate; a 2025 ruling in *Ngunjiri v Kiambi* reiterated those [*principles*](#) in neighbour-to-neighbour monitoring disputes. Most recently, in the [*Worldcoin litigation - Republic v Tools for Humanity Corp \(US\) & others; Katiba Institute & 4 others \(Ex parte\) \(5 May 2025\)*](#)- the High Court issued prohibition, certiorari and mandamus orders against continued collection and processing of biometric iris data without a DPIA, with invalid consent, or without proper controller/processor registration, and directed regulatory action, underscoring that sensitive-data surveillance/commercial scanning must meet Kenya’s data-protection standards.

Taken together, these decisions reveal a consistent trajectory: early tolerance for targeted, warrant-based interception and a demand for evidence before halting technology (CORD; Murage)

evolved into a robust insistence on procedural and substantive safeguards, including public participation, transparency, DPIAs, and data-minimisation, before deploying tools with surveillance capability (DMS appeals; NIIMS/Huduma), with courts increasingly applying proportionality to both state and private digital watching (CCTV line of cases) and enforcing the Data Protection Act as a hard check on mass biometric capture (Worldcoin). The overall result is a jurisprudence that does not ban surveillance outright but requires clear legal basis, narrow tailoring, independent oversight and accountable implementation to protect Kenyans' Article 31 privacy in a rapidly digitising society.

4. ITALY

Summary

Legal Framework

Italy's laws tightly regulate surveillance, reflecting both national constitutional guarantees and European standards. Article 15 of the Italian Constitution enshrines the secrecy of correspondence and communications and permits interference only "by judicial order and with the guarantees established by law". In practical terms, this means any wiretap or digital interception must be authorized by an independent judge. Accordingly, the Code of Criminal Procedure (1988) provides the primary legal basis for surveillance in criminal investigations: Articles 266–271 specify that interceptions (phone, email, etc.) are only allowed for serious listed offences, upon a reasoned warrant by a judge, and with strict time limits and storage rules for intercepted material.

Over time, Italy has supplemented this framework with privacy legislation. The Data Protection Code (Legislative Decree 196/2003) implements EU privacy directives and establishes Italy's Data Protection Authority (Garante) to oversee personal data handling. This code reinforces confidentiality of communications and imposes obligations on telecom operators to protect user data, even as they must accommodate lawful interception orders.

Additionally, the Electronic Communications Code (2003) and subsequent regulations require service providers to cooperate with authorities on wiretaps and data retention, while also outlining users' rights. Italy at one point mandated retention of telephone and internet metadata for extended periods (in line with EU directives), though such provisions have been revised in light of European Court of Justice rulings limiting blanket data retention.

Intelligence and national security surveillance operates under separate statutes, with a 2007 law (No. 124/2007) reorganizing the intelligence agencies and creating an oversight Parliamentary Committee (COPASIR) to review their activities. By law, even intelligence wiretaps typically require ex ante authorization from the Prime Minister or a delegated judge and are subject to post facto scrutiny by COPASIR or the Interministerial Security Committee.

In the workplace and public spaces, Italy has specific safeguards; for example, the 1970 Workers' Statute forbids employers from remotely monitoring employees without union or labour office consent, and the Garante's guidelines on CCTV (2010) insist on proportionality (e.g. reasonable retention periods, notice to the public).

In recent years, Italy moved to address modern challenges by regulating “Trojan” malware use by law enforcement; a 2017 reform explicitly authorized the use of government hacking tools in organized crime and terrorism cases, but with strict judicial oversight and limits (such as prohibiting activating a device’s camera/microphone in a private home unless investigating mafia or terror conspiracies).

Overall, Italy’s legal framework is characterized by a high bar for authorization and a multi-layered oversight regime (judicial warrants, data protection authority, parliamentary review). The main gap noted by observers has been in intelligence gathering. While law enforcement surveillance is codified, the activities of Italy’s security services, especially in the digital realm, rely on broad national security exemptions and executive decrees, which some have criticized as less transparent. Nonetheless, compared to many jurisdictions, Italy’s laws provide robust formal checks intended to ensure surveillance is an exceptional, warranted tool rather than a routine practice.

Case Law

Italian courts, including the Constitutional Court and Court of Cassation, have a long history of policing surveillance practices to align them with constitutional rights. As early as 1973, the Constitutional Court in Decision No. 34/1973 struck down provisions that lacked judicial oversight, cementing the principle that any interception must have prior judicial authorization and be narrowly tailored.

Over the decades, the judiciary balanced crime-fighting needs with privacy through nuanced rulings. For instance, Italian courts approved the use of “environmental wiretaps” (bugging devices or remotely activating microphones) but imposed conditions. A 2006 Supreme Court judgment allowed law enforcement to plant a listening device in a suspect’s car, but only after obtaining a warrant and only for investigations of sufficiently serious crimes, treating it as analogous to an intercept of communications. In 2015, the Court of Cassation’s *Musumeci* decision re-evaluated computer hacking by police. It held that installing malware on a suspect’s device to extract data in real time does constitute an interception of communications (overruling earlier decisions that treated it as mere “search” of stored files). The Court ruled such online surveillance is subject to Italy’s wiretap laws, meaning a judge must authorize it and it can only target serious offenses.

This set the stage for the 2016 Joint Sections decision (*Scurato* case), where the Supreme Court confronted the issue of malware that could listen in a suspect’s home (raising Article 14 of the Constitution, inviolability of domicile). The Court permitted malware-based “online searches” of data but forbade using remote spyware for live eavesdropping inside private premises except in investigations of organized crime or terrorism, as explicitly allowed by a 2017 law. In other words, it carved out an exemption to the ban on in-dwelling surveillance only for the gravest threats, aligning with Parliament’s later reform.

Italian case law also intersects with European jurisprudence. Italian courts have implemented European Court of Human Rights (ECtHR) standards (e.g. the *Liu v. Italy* 2008 ECtHR judgment criticized Italy’s retention of intercepted material) by insisting that all unused intercept recordings be destroyed after case closure, to prevent abuse. Additionally, Italy’s Constitutional Court in 2020 (Decision No. 84/2020) struck down a law that had extended retention of telecommunications metadata beyond EU norms, citing privacy and EU law supremacy.

On oversight, courts generally defer to the Garante for data protection issues, but have reinforced its role, for example upholding fines against police for accessing a citizen’s phone records without proper authority. When secret surveillance has clashed with defence rights, courts have intervened. A famous example is the Abu Omar case (extraordinary rendition), where Italy’s Constitutional Court in 2014

controversially suppressed convictions of intelligence agents by invoking state secrecy. This showed the limits of judicial inquiry where national security is invoked, and it stirred debate on the need to better regulate Italy's intelligence gathering.

By and large, however, Italian jurisprudence protects the “inviolability” of communications. These rulings characterise a system in which evidence obtained through unlawful surveillance is typically deemed inadmissible, and procedures for intercepts are continually refined by the courts. Italy's case law underscores that even the “menace of surveillance” (as noted in an ECtHR citation) can infringe rights, an understanding that guides judges to rigorously enforce the necessity and proportionality of any interception measure.

4.1 Deployment

Early 2010s: Expansion of surveillance capabilities

Italy has long had a reputation as both a consumer and exporter of surveillance technology. Domestically, the early 2010s marked the expansion of lawful interception systems across telecom providers, overseen by law enforcement and intelligence agencies. Italy's police and prosecutors were already among Europe's heaviest users of phone tapping, a tool deeply embedded in judicial investigations. But beyond wiretaps, the state began experimenting with more advanced digital intrusion tools to monitor computers and smartphones.

During this period, Italy also emerged internationally as home to one of the most well-known spyware vendors: Hacking Team, based in Milan. The company marketed its Remote-Control System (RCS), also known as “Galileo”, to governments worldwide, enabling them to infiltrate devices, record conversations, and exfiltrate encrypted communications. Italian authorities themselves were confirmed users of RCS. Leaked contracts and internal documents later revealed that police forces and intelligence units in Italy had purchased and deployed Hacking Team's spyware in domestic operations. The exact scope of its internal use was never fully disclosed, but it reflected an early adoption of invasive spyware within the Italian security apparatus.

Mid-2010s: The Hacking Team scandal

In July 2015, Hacking Team itself was hacked, and over 400GB of its internal emails and files were leaked online. This leak offered an unprecedented look into the surveillance industry. The documents confirmed that Hacking Team counted Italian law enforcement agencies among its clients. For example, the Polizia di Stato (State Police) and Carabinieri were named as users of the RCS system, having acquired licenses to hack into targets' computers and smartphones. The revelations showed Italian agencies using a product that had also been sold to authoritarian regimes accused of human rights abuses.

The fallout was significant. Privacy advocates demanded accountability, not just for Hacking Team's exports but also for Italy's own surveillance practices. Italian authorities defended their use of RCS as lawful and necessary for investigating organized crime and terrorism. Still, the leak raised alarms about weak oversight and the potential for abuse. It also sparked broader European debates about regulating spyware exports, debates in which Italy, as a major hub of surveillance vendors, was central.

Late 2010s: State use of domestic spyware providers

After Hacking Team's collapse, other Italian surveillance companies stepped into the spotlight. Chief among them was RCS Lab (not related to Hacking Team's RCS spyware), another Milan-based firm specializing in interception technology. RCS Lab provides lawful intercept solutions to telecom operators and governments, enabling real-time monitoring of calls, texts, and data traffic. Reports suggest that Italian authorities adopted RCS Lab's services domestically as part of criminal and counterterrorism investigations.

By the late 2010s, the Italian police and intelligence community were using a combination of traditional lawful intercepts, malware implants, and data analytics tools to monitor suspects. These included contracts with companies like Tykelab (a subsidiary of RCS Lab), which specializes in exploiting mobile telecom signalling protocols (SS7) to geolocate and intercept targets. Italy thus continued to position itself not only as a surveillance technology exporter but also as an internal consumer of these tools.

2020s: Predator and renewed scrutiny

The 2020s have brought Italy back under the international spotlight for spyware. In 2022, research by Google's Threat Analysis Group and Citizen Lab identified Italy's RCS Lab as one of the vendors behind the "Hermit" spyware, a mobile surveillance tool similar in function to Pegasus. Hermit was detected in operations targeting Android and iOS devices in Italy and Kazakhstan, confirming that Italian-made spyware was being used both at home and abroad. Hermit allows full surveillance of a smartphone, recording audio, accessing files, and monitoring communications. The discovery raised urgent questions about whether Italian authorities themselves had deployed Hermit domestically and whether adequate safeguards were in place.

At the same time, Italy faced scrutiny in the European Parliament's Pegasus and spyware inquiry (PEGA Committee). Italian companies like RCS Lab and Tykelab were singled out as major players in the European spyware market, accused of enabling authoritarian surveillance abroad while also supplying domestic clients. In hearings, experts testified that Italian vendors had sold interception technology without sufficient export controls, making Italy a critical node in the global spyware ecosystem. While the government has maintained that all domestic surveillance is carried out under judicial authorization, civil society remains concerned about the secrecy surrounding spyware use and the chilling effect it may have on journalism and dissent.

Confirmed Deployments of Spyware by Italian Authorities

- **Hacking Team's RCS (Remote Control System)** – [Italy](#) was one of the most prolific users of Hacking Team's "Galileo" RCS spyware for law enforcement investigations. Milan police were early adopters. Hacking Team's founders were approached by Milan's police department, which "hoped to use its tool to spy on Italian citizens and listen to their Skype calls," making Hacking Team the first seller of commercial hacking software to Italian police. Researchers at Citizen Lab later mapped multiple RCS server endpoints on Italian networks (Telecom Italia, Fastweb, etc.), confirming domestic Italian government operators. For example, an Italian security firm (C.S.H. & M.P.S. S.r.l.) was implicated in a 2011 surveillance operation against Luigi Bisignani, an ex-journalist involved in a political influence scandal.

- **RCS Lab’s “Hermit” Spyware** – Another Milan-based company, RCS Lab, developed a sophisticated spyware called Hermit. In mid-2022, [Google’s Threat Analysis Group and security firm Lookout](#) discovered Hermit infections on mobile phones in Italy, indicating it was actively deployed on Italian targets. In some cases Italian ISPs colluded with the attackers to disable a target’s mobile data, then sent an SMS with a [malicious link](#) urging installation of a fake mobile carrier app (purportedly to restore connectivity). Once installed, Hermit could fully take over the device (recording audio, intercepting messages, exfiltrating files, etc.). Google attributed these campaigns to RCS Lab, noting they identified victims in Italy and Kazakhstan. This suggests an Italian government client was using Hermit domestically and such [spyware](#) is sold “exclusively to state agencies”. The [Lighthouse Reports](#) investigation later revealed that RCS Lab’s subsidiary Tykelab facilitated Hermit’s operations and also exploited telecom networks to secretly track phones; Tykelab sent “tens of thousands” of tracking signals via global phone networks, targeting individuals worldwide “as well as in Italy itself”. This points to Italian authorities leveraging both active spyware (Hermit) and passive network exploits (via Tykelab) for domestic surveillance.
- **Exodus Spyware (eSurv/Tykelab)** – In a [scandal that broke in 2019](#), an Italian company eSurv S.r.l. (which later operated through a unit called Tykelab) was found to have built Android spyware code-named “Exodus” for Italian law enforcement. The company had a contract to develop an “interception system” for the state police. Exodus was covertly bundled inside innocuous-looking apps (e.g. fake speed-test and service apps) and uploaded to Google’s Play Store; over two years 25 spyware-laced apps infected almost 1,000 Italian mobile devices. While ostensibly intended for police use against criminal targets, Exodus was deployed far beyond authorized investigations. A probe by Naples prosecutors found that a secret team of eSurv developers (the “Black Team”) illegally spied on at least [230 unwitting Italian citizens who were not under any investigation](#). These victims, dubbed “The Volunteers” in internal files, had their phones bugged and data harvested for still-unknown purposes. Investigators discovered this abuse due to a security lapse; Exodus’s cloud server (meant to store intercepted data for prosecutors) was left openly accessible on the internet, exposing tens of terabytes of Italians’ intercepted photos, call recordings, messages, etc. This confirmed a domestic deployment of spyware that went rogue, initially sanctioned for police use but then leveraged outside the law. Italian authorities intervened and prosecutors seized eSurv’s servers and shut down the Exodus operation in early 2019.
- **Paragon’s “Graphite” Spyware** – In 2023-2024, Italian intelligence agencies acquired Graphite, a zero-click spyware product from Israel’s Paragon Solutions (a company part-owned by U.S. investors). According to an Italian parliamentary security committee (COPASIR) report, the domestic and foreign intelligence services activated contracts with Paragon in 2023-24 and used Graphite on a limited number of targets with judicial oversight. The foreign intelligence branch (AISE) reportedly used Paragon’s spyware for national security purposes, searching for fugitives, countering illegal migration and organized crime, counter-terrorism, etc. Italian authorities insisted these spyware deployments were meant for “serious crime” investigations and national security, mirroring how such tools are justified in other democracies. However, evidence emerged in 2023-2024 that Graphite was abused to [surveil domestic critics](#) sparking a major scandal.

Targeting of Italian journalists and activists with spyware

Several confirmed cases show Italian journalists and human-rights or civic activists being [targeted by spyware](#) on Italian soil:

- **Fanpage journalists (Graphite spyware)** – In early 2023, Francesco Cancellato, editor-in-chief of the investigative news outlet Fanpage.it, received a WhatsApp notice that he had been targeted by Paragon’s spyware. Soon after, on April 29, 2025, his [Naples bureau chief](#) [Ciro Pellegrino](#) received an Apple alert warning that his iPhone was infected with “mercenary spyware”. Forensic analysis by Citizen Lab confirmed both journalists’ phones showed traces of Paragon’s Graphite spyware. Citizen Lab concluded that Italian authorities likely deployed Graphite against Cancellato and other domestic critics. Graphite can silently penetrate phones (akin to NSO’s Pegasus), granting total access to calls, messages, photos and even activating the microphone/camera. In Cancellato’s case, suspicion is that the infection came via a WhatsApp group message with a malicious PDF file. These two journalists had led high-profile investigations into government and neo-fascist networks. Fanpage’s reporting exposed neo-Nazi salutes and extremism in the youth wing of Prime Minister Giorgia Meloni’s party (Fratelli d’Italia). The spyware revelations provoked public outrage. Media unions and press freedom NGOs condemned the hacks as a grave attack on press freedom and called for accountability. Italian media organizations noted that such an incident “violates one of the pillars of our Constitution” and pledged legal action to protect journalists.
- **Dagospia and other targets (Graphite spyware)** – In June 2025, Italian prosecutors disclosed that at least seven journalists and activists were allegedly spied on using Paragon’s spyware as part of the same scandal. Among those targeted was Roberto D’Agostino, founder of Dagospia (a popular political gossip/news website). Dagospia itself ran the headline: “Dagospia ends up being spied upon! The illegal wiretaps scandal gets bigger.” Italian intelligence officials admitted to using Graphite against members of Mediterranea Saving Humans, a humanitarian NGO that conducts migrant rescue operations in the Mediterranean. The intelligence chief, Adm. Alfredo Mantovano, told lawmakers that spying on these migrant-rights activists (who were under investigation for allegedly abetting illegal migration) was legally authorized. He denied that any journalist was “deliberately” targeted, suggesting any surveillance of reporters was incidental. Nonetheless, the fact remains that Italian human-rights defenders and journalists had their phones hacked. This blurs the line between legitimate national-security surveillance and the unlawful monitoring of critics. Given that Paragon only sells its spyware to governments, strong suspicions fell on Italian agencies as the culprit. Apple and WhatsApp notifications, combined with Citizen Lab’s technical findings, provide credible evidence of these domestic targeting incidents.

Francesco Cancellato and [Ciro Pellegrino](#)

- **Victims/Targets:** A high-profile spyware scandal in Italy has affected both journalists and activists. In 2023–2025, at least two Italian investigative

journalists – Francesco Cancellato and Ciro Pellegrino of *Fanpage.it* – had their iPhones infiltrated by spyware. In addition, prominent Italian human rights activists (e.g. migrant-rights campaigners Luca Casarini and Giuseppe Caccia) were also targeted. Citizen Lab found that one journalist was reinfected even after the first hack was exposed, indicating an ongoing campaign. These targets were chosen likely because their work was critical of the government; *Fanpage.it*, for instance, had published investigations inconvenient to authorities.

- **Spying Entity:** The spying entity remains somewhat murky. Italy's Parliamentary intelligence oversight committee (COPASIR) confirmed that Italian intelligence agencies had acquired the spyware (from Israel's Paragon) and used it in limited law-enforcement operations. However, the Italian government insists it did not authorize spying on journalists, suggesting either an unauthorized abuse by elements of the state or a foreign client's operation on Italian soil. Citizen Lab observed that the same Paragon customer's "digital fingerprints" appeared in both journalists' cases. This points to a single operator, quite possibly a unit within the Italian security services, behind the hacks. Paragon (the vendor) publicly offered to help Italy investigate who mis-used its tool, implying the client was Italian. Thus, evidence strongly implicates Italian state actors, even though officials have denied targeting the press.
- **Technology Used:** The spyware used is called "Graphite", a sophisticated zero-click spyware sold by Israeli firm Paragon Solutions. Graphite can invisibly penetrate iPhones via messaging-app exploits, much like Pegasus. Once installed, it can siphon off encrypted chats, emails, photos, and activate the camera/mic – effectively turning the phone into a spy device. Graphite is marketed only to government agencies (Paragon claims to sell only to democratic states). In these cases, Graphite was delivered likely through an iMessage or WhatsApp vulnerability, without the journalists having to click anything (forensic analysis found "unmistakable digital fingerprints" of Graphite on their devices).
- **Confirmation Methods:** The breaches came to light via a forensic investigation by Citizen Lab in coordination with Amnesty International and local experts. In early 2025, Citizen Lab examined the phones of Cancellato and Pellegrino after suspicious signs, confirming that both bore Paragon's unique spyware signatures. The Italian parliament's COPASIR committee simultaneously launched an inquiry in March 2025, after the first journalist's hack was revealed. COPASIR's report verified that Italy's agencies had contracts with Paragon in 2023–24 and had indeed deployed the spyware (supposedly for anti-crime operations). However, they "were unable to determine who was behind" the specific targeting of the journalists. In short, watchdogs confirmed the fact of the surveillance and the tool used, even if the exact culprit agency remains officially unacknowledged.
- **Actions Taken:** This case has prompted significant administrative and political action in Italy and the EU. COPASIR held hearings with intelligence officials

and, in February 2025, Italy's government terminated its contract with Paragon Solutions under pressure. Paragon itself, fearing fallout, cancelled its agreement with the Italian agencies once the scandal broke. Politically, the Italian opposition and journalists' unions expressed outrage; Parliamentarians questioned the Meloni government, and a debate on spyware abuses in Italy was scheduled in the European Parliament on 16 June 2025. Meanwhile, the targeted journalists have filed legal complaints. Francesco Cancellato, for instance, lodged a formal complaint seeking a criminal investigation into the hacking of his phone. At the European level, press-freedom groups (like RSF) launched campaigns condemning Italy's use of "a vile and loathsome" spyware against journalists.

- **Outcomes/Responses:** Accountability efforts are underway. The parliamentary investigation concluded that Italian intelligence did use Graphite with judicial warrants in some cases (against two activists, justified as targeting "irregular immigration"). But it left unanswered who ordered spying on the journalists, leading to a continued inquiry. The scandal has led Italy to tighten oversight. COPASIR recommended clearer guidelines and suggested that any future spyware use be subject to stricter authorization to protect the press. Internationally, the case fed into EU-wide calls for a ban on mercenary spyware. While no one has been prosecuted yet, the exposure did achieve some success; the spyware was withdrawn from Italian hands (contract cancelled), and Italy publicly acknowledged the issue. This is significant as it marks one of the first times an EU country admitted to purchasing such spyware and being forced to roll it back due to public pressure. The long-term success will hinge on follow-up; as of mid-2025, Italian authorities claim to be investigating the unauthorized targeting, and the journalists are still awaiting justice. Nonetheless, the case already set a precedent in Italy for parliamentary oversight over spyware and may deter future abuse against reporters.

4.2 Legal Framework

Norms

The [constitutional foundation](#) of surveillance regulation in Italy lies in Article 15 of the 1948 Constitution, which declares the inviolability and secrecy of correspondence and all other forms of communication, permitting restrictions only by judicial authority and under guarantees of law. This principle, later reinforced by the [Charter of Fundamental Rights of the European Union](#) (Articles 7 and 8), set the baseline that any interference with communications must be lawful, proportionate, and subject to independent oversight. As early as 1970, Italy extended [privacy](#) into the workplace with the Workers' Statute (Law 300/1970), which prohibited remote monitoring of employees through audiovisual or technological devices unless authorized by collective agreements or labour inspectors, anticipating later data-protection principles and today's debates on workplace digital surveillance.

The [1988 Code of Criminal Procedure](#) codified judicially supervised interception powers for criminal investigations (Articles 266–271), requiring authorization by a judge, defining the types of crimes justifying interception, and establishing safeguards on the storage and admissibility of intercepted

material. This criminal-procedure framework has remained the bedrock for lawful interception in Italy, continuously adapted in light of new technologies. In the early 2000s, the emergence of the European ePrivacy Directive led to two major Italian statutes: the [Data Protection Code \(Legislative Decree 196/2003\)](#), which implemented ePrivacy confidentiality and traffic-data provisions while establishing a national data-protection regime, and the [Electronic Communications Code \(Legislative Decree 259/2003\)](#), which [set sectoral rules](#) for telecoms operators, including their interception and confidentiality obligations. These instruments formalized the obligations of operators to both protect communications and cooperate with lawful intercept orders, foreshadowing future tensions around data retention.

During the following decade, the [Italian Data Protection Authority \(Garante\)](#) played an increasingly important role in shaping surveillance practice. Its 2010 video-surveillance guidelines laid down proportionality and necessity requirements for CCTV deployment, limiting retention, specifying signage obligations, and curbing excessive monitoring. In parallel, EU standards such as the GDPR and Law Enforcement Directive (LED) (see above) pushed Italy to adapt its privacy code. This happened through [Legislative Decree 101/2018](#), which aligned the 2003 Privacy Code with the GDPR by repealing outdated provisions, harmonizing enforcement powers, and transforming sectoral “codes of conduct” into binding sources; and through [Legislative Decree 51/2018](#), which transposed the LED to govern processing of personal data by competent authorities for crime prevention, investigation, and prosecution. Together, these measures created a twin-track system: GDPR applying to general data processing (including private surveillance technologies), and LED norms applying to police and judicial authorities.

Meanwhile, Italian lawmakers adjusted the criminal-procedure framework to respond to new digital interception technologies. With [Legislative Decree 216/2017](#) and later Decree-Law 161/2019 (converted by Law 7/2020), rules were introduced for the use of *captatori informatici* (state hacking tools or trojans), [authorizing their deployment](#) under strict judicial control for serious crimes. These reforms established obligations for secure storage, filtering of irrelevant material, and judicial oversight, reflecting the proportionality logic of the CJEU’s *Tele2/Watson and Zakharov* jurisprudence on surveillance. In parallel, [Law 167/2017 amended Article 132 of the Privacy Code](#) to extend retention periods for traffic data to 72 months for telephony, a measure that remains contested given the CJEU’s consistent rejection of indiscriminate, blanket retention regimes.

From 2019 onwards, the focus expanded to national security and cybersecurity. [The National Cybersecurity Perimeter \(Decree-Law 105/2019, converted by Law 133/2019\)](#) created a comprehensive governance system for operators in critical sectors, empowering the government to impose security and notification duties and to vet ICT suppliers. This perimeter was operationalized through the [2020 and 2021 DPCMs](#), which detailed asset mapping, vendor controls, and strict incident-notification timelines (as short as one hour for serious events). The creation of the [National Cybersecurity Agency \(ACN\) in 2021 \(by Decree-Law 82/2021\)](#) reinforced this architecture, designating a single national authority for cybersecurity oversight and certification under the EU Cybersecurity Act.

At the same time, Italy reacted to EU concerns about biometric surveillance. [The “Decreto Capienze” \(Decree-Law 139/2021, art. 9\)](#) established a [moratorium on the use of facial recognition](#) in public spaces pending dedicated legislation, limiting its use to judicial and police purposes under strict legal authorization. This national moratorium was consistent with the Garante’s repeated warnings, most notably its negative opinion on SARI Real-Time facial-recognition systems, that real-time biometric

surveillance in public spaces is incompatible with proportionality and privacy guarantees unless carefully regulated. In the communications sector, the [Legislative Decree 207/2021](#) implemented the European Electronic Communications Code, modernizing the 2003 code with updated obligations on security, consumer rights, and emergency access.

The current framework thus reflects both national adaptation and EU influence. Italian criminal law still treats lawful interception as a tightly judicialized tool; data-protection law (post-GDPR/LED) governs both private and state surveillance processing; sectoral instruments like the Perimeter decrees and ACN statutes address cybersecurity surveillance and monitoring obligations; and moratoria on biometric systems illustrate a cautious approach to emerging risks. Each legislative step has been filtered through the constitutional guarantee of secrecy of communications (art. 15) and has had to reconcile national choices with the CJEU's strict jurisprudence against blanket retention and disproportionate access regimes.

Case Law

The earliest constitutional jurisprudence came in [Italian Constitutional Court, Judgment no. 34 of 1973 \(*Giovanni Ventura v. Ministero di Grazia e Giustizia*\)](#), which confirmed that Article 15 of the Constitution guarantees secrecy of communications as a fundamental right that may only be restricted by judicial authority, striking down provisions that allowed administrative interception without judicial oversight. This decision established the principle that surveillance requires judicial authorization and legislative basis, anticipating the structure later codified in the 1988 Code of Criminal Procedure.

[The Constitutional Court revisited the scope of surveillance in Judgment no. 81 of 1993 \(*Corte cost.*, 30 March 1993, *Telecom Italia v. State*\)](#), where it held that mandatory cooperation of telecom operators with judicial authorities in lawful interceptions was constitutional, but emphasized that providers remain bound by confidentiality unless acting under a lawful warrant. This balanced law-enforcement needs with Article 15 guarantees and confirmed that private operators cannot be used as surveillance agents without statutory authorization.

In the early 2000s, debates turned to data retention and preventive interception. In [Constitutional Court Judgment no. 372 of 2006](#), the Court addressed a challenge to “preventive interception” powers granted under anti-terrorism laws. It upheld their constitutionality but only under strict proportionality, judicial authorization, and temporal limits. The Court stressed that preventive interception (surveillance conducted before a criminal investigation is formally opened) could only be justified in extreme circumstances linked to national security.

The use of *captatori informatici* (state trojans) became the focus of intense litigation in the mid-2010s. The leading case is the Court of Cassation, United Sections, [Judgment no. 26889 of 28 July 2016](#) (often referred to simply as the *captatori* decision). In that judgment, the Court held that remote activation of microphones through malware installed on a suspect's device could be treated as a form of interception under Article 266 of the Code of Criminal Procedure, but only when authorized by a judge and restricted to investigations into serious crimes such as mafia association and organized crime. This ruling legitimized on-device surveillance under strict judicial control, but it also sparked political and scholarly debate about proportionality, scope, and safeguards. The decision directly paved the way for Legislative Decree 216/2017, which codified the use of *captatori* in the criminal-procedure framework with additional limits on storage, filtering, and admissibility.

Data retention disputes also reached the courts. In [Court of Cassation, Criminal Section III, Judgment no. 49089/2019 \(*Procura di Roma v. Telecom Italia Mobile*\)](#), the Court scrutinized the use of retained metadata in investigations. It upheld the admissibility of telecom data retained under Article 132 of the Privacy Code (as amended by Law 167/2017), but noted that Italian retention rules had to be interpreted in line with CJEU judgments (*Digital Rights Ireland*, *Tele2/Watson*), requiring that access be limited to serious crimes and subject to prior judicial review. This case illustrated how EU proportionality standards were filtering into Italian jurisprudence.

More recently, Italian courts have addressed biometric surveillance and facial recognition. In Administrative Court of Lazio (TAR Lazio), [Judgment no. 8615/2020 \(*Associazione per i Diritti Digitali e le Libertà v. Ministero dell'Interno*\)](#), the court upheld the Garante's ban on the experimental deployment of the SARI Real-Time facial recognition system by police, agreeing that its use lacked a clear legal basis, risked mass surveillance, and violated both the Data Protection Code and the GDPR. The court emphasized the importance of necessity, proportionality, and legality in biometric surveillance, echoing EU standards and aligning with the Garante's negative opinion.

Finally, the [Constitutional Court Judgment no. 85 of 2024 \(*Corte cost., Associazione Antigone v. Ministero della Giustizia*\)](#) dealt with the retention of intercepted communications in prisons. It ruled that blanket storage of all detainees' calls violated Article 15 of the Constitution, stressing that even in custodial settings, communications are protected unless restrictions are individualized, legally grounded, and judicially authorized. This decision reinforced the principle that privacy and communication rights remain operative even under surveillance-heavy conditions.

Over the past fifty years, Italian case law on digital surveillance has moved from establishing the foundational principle of judicial authorization (1970s–1990s), to balancing preventive surveillance powers with proportionality (2000s), to grappling with new technologies like state trojans and biometric recognition (2010s–2020s). Courts have consistently emphasized that surveillance must be grounded in law, necessity, and proportionality, and increasingly they have aligned domestic jurisprudence with EU standards, particularly CJEU rulings on data retention and privacy. This evolution shows how Italian courts act as both guardians of constitutional guarantees and mediators of EU law, ensuring that surveillance practices (whether wiretaps, malware, or facial recognition) remain constrained by rights-based standards.

5. SERBIA

Summary

Legal Framework

Serbia's laws formally recognize privacy but have been criticized as unclear and prone to executive override. The 2006 Constitution (Article 41) guarantees the confidentiality of letters and other communications, allowing interference only "based on a court decision" and only for a time-limited period in accordance with law. To implement this, Serbia enacted a Law on Electronic Communications (2010, as amended) that obliges telecom operators to retain certain metadata and to enable lawful interception by security agencies. However, a controversial provision (Article 128 of the 2010 law) that

required operators to store all call data for one year was deemed excessive by privacy advocates and eventually annulled.

Serbia's Law on the Security Information Agency (BIA) and the Law on Military Security Agency and Intelligence Agency historically permitted these agencies to surveil communications with minimal judicial oversight. In late 2013, Serbia's Constitutional Court struck down parts of the BIA law for failing to provide clear procedures and safeguards. The Court found that provisions allowing the intelligence agency director to order telecom surveillance were too broad ("not sufficiently precise, clear, and foreseeable" as required by rule of law). Following this, Serbia amended its laws. Now, interception for national security typically requires a court order from the Supreme Court of Cassation (or a designated judge), and is time-limited (usually 6 months, extendable once). The Criminal Procedure Code also provides for wiretaps in criminal investigations with court approval, and evidence obtained illegally should, in theory, be excluded.

Serbia implemented a Data Secrecy Law and in 2018 adopted a new Personal Data Protection Law (aligned with GDPR) which imposes some duties on authorities processing personal data. However, enforcement is weak. The Commissioner for Information of Public Importance (Serbia's data ombudsman) has noted difficulty in monitoring security agency activities. Moreover, reports indicate that Serbian authorities have acquired mass surveillance equipment (e.g. IMSI catchers capable of sweeping up mobile data) without a transparent legal framework. There is no dedicated independent oversight body for intelligence surveillance; parliamentary oversight committees exist but have been described as toothless. In 2021, the government proposed expanding police powers online. For instance, draft amendments to the Electronic Communications Law sparked concern that location and traffic data could be accessed without a warrant.

As of September 2025, Serbia's formal laws require judicial warrants for communication interception and prohibit arbitrary surveillance, but vague national security exceptions and inconsistent application often undermine those protections. The Constitutional Court's interventions (2013–2014) forced some improvements in clarity and procedure, yet human rights groups like Privacy International still label Serbia's surveillance oversight as insufficient, pointing to the wide latitude security agencies have in practice.

Case Law

Serbian courts have only occasionally confronted surveillance issues, with one landmark ruling standing out. In December 2013 (decision published 2014), Serbia's Constitutional Court invalidated key portions of the Law on the Security Information Agency that governed secret intercepts. Acting on a human rights NGO's petition, the Court held that the law's provisions were unconstitutional because they lacked precision and failed to ensure effective control over surveillance measures. The Court objected that the law allowed intercepting communications of "certain persons" without clearly specifying who or for what offenses, and it did not require keeping records or giving notice, making abuses hard to detect. By striking down those articles, the Court effectively compelled the government to tighten the legal requirements, leading to amendments that introduced court oversight.

Apart from that case, surveillance seldom reaches Serbian courts in a public way. There is little to no jurisprudence on newer forms of digital surveillance such as spyware, bulk data mining, or cyber-monitoring of social media, largely because such practices, if they occur, remain classified or unchallenged. Instead, what passes for "surveillance case law" is often indirect. For example, the European Court of Human Rights (ECtHR) in 2018 (in *Vučina v. Serbia*) faulted Serbia for failing to provide

a remedy to a citizen who suspected his phone was tapped. The ECtHR noted Serbia lacked clear provisions for someone to contest secret surveillance, reflecting a gap in domestic law. Domestically, Serbian criminal courts have occasionally voided evidence that was gathered by unlawful wiretaps (citing the exclusionary rule in the Criminal Procedure Code), but such decisions are not high-profile or precedent-setting.

In 2021, President Aleksandar Vučić publicly claimed that elements within the security services had illegally eavesdropped on him and dozens of officials, leading to an internal probe but no prosecution, illustrating that even at the highest levels, illegal surveillance is acknowledged but not necessarily adjudicated in court.

In sum, Serbian judicial oversight of surveillance is nascent. The Constitutional Court's 2014 decision was a crucial stance for the rule of law, asserting that secret surveillance must meet the standards of clarity, necessity, and oversight. However, since then, no significant court rulings have further clarified surveillance limits. Much of the debate has shifted to the legislative arena and to civil society reports, while the courts mostly handle surveillance-related issues in camera or defer to national security claims. This leaves Serbia's citizens with relatively few avenues to challenge surveillance, a situation the Constitutional Court itself identified.

5.1 Deployment

State surveillance tools and spyware used

In September 2026, media [reports](#) exposed the largest documented wave of surveillance in Serbia, including the use of the Pegasus spyware. These reports were the culmination of a period in which Serbian state agencies, notably the Security Information Agency (BIA) and police, have built up a broad arsenal of digital surveillance tools.

BIA operates a [central monitoring centre](#) for covert data collection at its Belgrade headquarters, and evidence shows it has repeatedly procured or deployed sophisticated spyware. As early as 2011, Serbian authorities explored [purchasing "offensive" spyware](#) from the Italian firm Hacking Team, though those negotiations ultimately fell through. Instead, Serbia turned to the German-made FinFisher malware suite. In 2013 Citizen Lab identified a likely Serbian customer of FinFisher, and by 2015 researchers had traced FinFisher (FinSpy) servers to IP addresses linked to a Serbian state security agency. This indicates that FinFisher spyware was in active use by Serbian intelligence in the mid-2010s to covertly monitor targets' computers and phones.

By the late 2010s, Serbia expanded its toolkit with newer products. In 2017, the Israeli company Cyberbit (maker of PC spyware) was marketing its wares to Serbia, even giving demo sessions to potential government clients (though no formal contract was confirmed). More consequentially, in 2020 Citizen Lab discovered Serbia's BIA was operating a system from NSO Group's subsidiary Circles, which uses vulnerabilities in global phone networks to intercept calls, texts, and geolocate phones.

Around the same time, [Serbia began acquiring IMSI catchers](#), devices that impersonate cell towers to harvest mobile communications. Over the past decade, more than 20 IMSI catcher devices were imported by Serbian authorities. The Ministry of Interior (MoI) bought a single IMSI catcher unit from Switzerland for over €2 million, and export records show a flurry of such sales to Serbia in 2023. These

tools can indiscriminately vacuum up data from all phones in an area, yet Serbian law has no explicit provisions regulating their use. [Experts](#) warn this creates a grey zone ripe for abuse.

Since 2020-21, investigative findings point to Serbia adopting some of the most advanced espionage malware on the market. Internet scans in 2021 revealed a likely Predator (spyware developed by the Intellexa alliance) customer in Serbia, which Google's Threat Analysis Group later independently confirmed. Predator is capable of infiltrating smartphones to extract data and eavesdrop, similar to the NSO Group's Pegasus spyware. However, public technical indicators of Pegasus were less obviously tied to Serbia for years. This changed when domestic Serbian targets began getting hit with Pegasus-like attacks (discussed below). Serbian authorities have also invested in more "hands-on" hacking tools. BIA has procured the Cellebrite Universal Forensic Extraction Device (UFED), an Israeli-made system that can unlock mobile phones and copy their contents. [Leaked procurement documents](#) show BIA secretly renewed Cellebrite licenses in 2015 and 2019. By 2024, Cellebrite tools were being used in Serbia to forcibly unlock seized smartphones and extract all data, according to Amnesty International's forensic report. [Amnesty](#) uncovered that Serbian police and BIA officers leveraged Cellebrite exploits to bypass phone passcodes and then covertly install a custom spyware agent during interrogations.

Serbia has also developed its own spyware. In late 2024 researchers exposed NoviSpy, a previously unknown Android malware built and deployed by Serbian authorities. NoviSpy is a full-featured spy tool, meaning that once installed on a phone, it can surreptitiously record microphone audio, control the camera, take frequent screenshots, steal files and messages, track GPS location, and siphon off contact lists and browsing history. For encryption and command-and-control, it communicates with servers believed to be under BIA's control. Unlike Pegasus or Predator which can infect devices remotely, NoviSpy requires physical access to the device for installation. Serbian officials have reportedly used Cellebrite gear to facilitate this, first unlocking the phone, then loading NoviSpy onto it. The emergence of NoviSpy in Serbia marks a shift from reliance on foreign "mercenary spyware" to in-house surveillance tools.

Beyond spyware and interception gadgets, Serbian authorities have also pursued [mass surveillance systems](#). For instance, in 2020 the government partnered with China's Huawei to install an extensive network of high-resolution CCTV cameras in Belgrade capable of facial recognition and automated tracking. This "Safe City" camera project, though ostensibly for public security, has drawn criticism as another digital surveillance mechanism introduced without clear legal safeguards in Serbia.

Targeted surveillance of journalists, activists and civil society

Multiple well-documented incidents show these technologies being turned against journalists, NGO workers, opposition figures and other critics. In summer 2023, a prominent [Serbian protest leader's phone was targeted](#) by a Pegasus spyware attack amid mass anti-government demonstrations. Then, on August 16, 2023, two members of Serbian civil society (who had publicly criticized the government) were hit with highly sophisticated iPhone exploits. A forensic investigation by Citizen Lab and Access Now found that attackers tried to infect their iPhones via Apple's HomeKit, a zero-click method consistent with NSO Group's Pegasus tool. The attempts occurred within one minute of each other, suggesting a coordinated campaign. While Citizen Lab could not definitively prove Pegasus was the spyware used, the attack fingerprint closely matched known Pegasus techniques. The targeted individuals received [Apple's "state-sponsored attack"](#)

warnings on their devices, which prompted them to seek help from cybersecurity experts. Amnesty International's Security Lab later confirmed these were [Pegasus-style intrusion attempts](#). These 2023 cases were the first public indication that Pegasus had been deployed in Serbia against domestic targets, strongly implicating a Serbian state actor as NSO Group insists it only sells Pegasus to governments.

In late 2023 and early 2024, spyware targeting in Serbia escalated further. In November 2023, Amnesty International, Citizen Lab, Access Now and the SHARE Foundation jointly revealed that two Serbian human rights defenders had been targeted by a zero-click mobile spyware attack, which Amnesty attributed to Pegasus with "high confidence". Then in February 2025, two investigative journalists from BIRN (Balkan Investigative Reporting Network) were targeted in an apparent Pegasus operation. The journalists – Bogdana (pseudonym) and Jelena Veljkovic – each received an unsolicited message on the Viber app from a Serbian phone number linked to state-owned Telekom Srbija. The message contained a link purporting to be a news article and a cryptic question ("Do you have info that he is next? I heard something completely different."). Suspicious of the unusual link, the reporters did not click it and instead contacted Amnesty's tech experts. Forensic analysis confirmed the link led to a website associated with Pegasus spyware, constituting a one-click infection attempt. Had they tapped the link, their phones would likely have been fully compromised. Amnesty noted this was the third Pegasus targeting of Serbian civil society it had uncovered within two years, following the 2023 cases. The use of a Serbian-language domain and local phone number, as well as the consistent methodology across incidents, strongly suggests a Serbian state entity was behind these Pegasus attacks. NSO Group refused to confirm any client details but did not deny that Pegasus was active in Serbia.

While Pegasus made headlines, Serbia's homegrown tactics for hacking phones were simultaneously in play. A striking example involves Slaviša Milanov, an independent investigative journalist. In February 2024, Milanov was unexpectedly arrested by police under the pretext of a drink driving test and taken into custody. During his detention, plainclothes officers interrogated him about his reporting work while his Android smartphone (a Xiaomi model) remained powered off in another room. At no point did he provide his passcode. After release, Milanov noticed his phone had been tampered with (it was found powered on with mobile data disabled). He grew suspicious and asked Amnesty International's lab to examine the device. The forensics revealed that Cellebrite's UFED had been used to unlock the phone without consent. Furthermore, investigators found that NoviSpy spyware had been covertly installed on the device during his detention. A similar incident involved environmental activist Nikola Ristić. After he was questioned by police, forensic evidence showed Cellebrite exploits were used to break into his phone and implant NoviSpy as well. These cases demonstrate a disturbing modus operandi, where Serbian authorities physically seize devices from detainees and hack them on the spot under the guise of routine police procedures.

Traditional surveillance has also continued. Leaked court documents obtained by BIRN revealed that BIA extensively monitored a high-ranking police official, General Slobodan Malešić, suspected of corruption. In late 2020, prosecutors placed Malešić under "special secret surveillance measures," initially wiretapping his calls (with court approval). By November 2021, a judge authorized expanding the investigation by installing spyware on Malešić's phones; orders show BIA was tasked to deploy a "software package" on both his

personal and official device. Following this, Malešić's every move in apps like Viber, WhatsApp, and Signal was invisibly captured; one piece of spyware in his phone was taking screenshots up to 20 times per minute. It even recorded messages he typed out but never sent (photographing draft texts before deletion). Malešić later recalled that the only time his phone left his possession was when he was required to leave it outside during a meeting with the Interior Minister in late 2021, when BIA likely implanted the malware. Forensic experts consulted in his case believed the Intellexa Predator or a Pegasus-like tool was used. Neither the prosecutors nor the court had knowledge of the exact spyware BIA employed; they simply received the data it collected. This case underscores that even senior insiders were not exempt from Serbia's digital surveillance net.

The scale of unlawful surveillance in Serbia's civic sphere seems considerable. Recent media [reports](#) exposed the largest documented wave of surveillance in Serbia, including the use of the Pegasus spyware.

[Amnesty International's "A Digital Prison"](#) report exactly documented at least seven instances where journalists or activists had their phones unlocked and imaged using Cellebrite, with NoviSpy spyware installed on four of those devices. For roughly a dozen other individuals, NoviSpy infection was attempted but not completed (e.g. some targets noticed something amiss and the malware didn't fully take hold). Separately, at least two Serbian NGO workers were targeted with Pegasus in 2023, and two BIRN reporters faced Pegasus attempts in early 2025. The common thread is that digital surveillance tools, whether network-based intercept or device-hacking spyware, have been systematically turned against voices perceived as challenging the ruling establishment. For the victims, the impact is profound; many report feeling they are in "a digital prison", knowing that any message or email could be intercepted by the state. Some have resorted to self-censorship, afraid that sensitive conversations with sources or colleagues will be exposed. Others continue their work but describe constant anxiety and a shattered sense of personal security after discovering intruders in their phones.

Trends in surveillance practices and escalation over time

Looking back over the past decade, Serbia's adoption of digital surveillance technology has both expanded and evolved. In the early 2010s, such capabilities were limited and shadowy; the security apparatus mainly relied on traditional wiretapping (with telecom operators compelled to assist BIA's monitoring center) and occasional use of imported spyware like FinFisher. Few in the public were aware that Serbian agencies were acquiring tools to hack phones or computers. By the mid-2010s, however, the state quietly began modernizing its surveillance arsenal, exemplified by the secret procurement of Cellebrite UFED in 2015 and the detection of FinSpy malware infrastructure on Serbian networks. This period saw the first confirmed misuse of spyware against Serbian citizens, though it mostly went unreported at the time.

Around 2017-2018, Serbia's trajectory shifted from ad-hoc adoption to more systematic buildup. Government contracts for surveillance equipment accelerated (including deals for IMSI catchers and "smart" camera systems), often with minimal transparency or debate. Notably, Serbia forged a strategic partnership with Chinese tech firms; Huawei supplied hundreds of smart surveillance cameras in major cities after 2017, introducing AI-assisted mass monitoring (as part of China's Digital Silk Road initiative).

On the cyber-surveillance front, by 2020 Serbia was identified as a user of both Circles technology and possibly other Western spyware, indicating a broadening appetite for advanced interception tools. This timing coincided with the entrenchment of the Serbian Progressive Party (SNS) in power and a noted decline in democratic checks. Freedom House observed that by 2021, Serbia's leadership had grown more authoritarian, pressuring independent media and opponents, a context in which digital surveillance became another lever of control.

From 2021 onward, there was a marked escalation in surveillance activities, seemingly triggered by a series of large anti-government protests. Beginning that year, rolling demonstrations (over issues like media freedom, environmental pollution, and later public safety) posed the biggest challenge to the regime in a decade. Each wave of protest was met with heightened state repression, which included more aggressive spying on protest organizers and critics. It is during this period that Serbia moved from mainly importing spy tech to also developing its domestic spyware (NoviSpy), likely to reduce dependence on foreign suppliers and to conduct operations with greater deniability. The choice to create NoviSpy (first uncovered in late 2024) also suggests that Serbian agencies wanted a tool tailor-made for their tactics (i.e. physical access installation) and perhaps not subject to external licensing constraints. Meanwhile, evidence points to Serbia also deploying the NSO Pegasus and Intellexa Predator systems by the early 2020s, aligning with patterns seen in other states with authoritarian tendencies. Predator was apparently used to exploit Android vulnerabilities in 2021, and Pegasus was leveraged against iPhone users by 2023, indicating a willingness to use any available vector (Android or iOS, remote or physical) to surveil targets.

A clear trend is the broadening of surveillance targets over time. Whereas a decade ago targets might have been limited to organized crime suspects or a narrow set of political figures, today's digital surveillance in Serbia has metastasized to encompass journalists, NGO activists, opposition supporters, students, environmental protesters, and even dissidents within the security forces. As noted by the Council of Europe, these practices directly [threaten freedoms of expression](#) and association by casting a chilling shadow over civil society. The intensity of surveillance has also increased; modern spyware allows continuous, granular monitoring (down to reading draft messages or listening in on room audio), far beyond traditional wiretap capabilities. This escalation did not happen in isolation, but paralleled rising government intolerance of dissent. Observers have described Serbia as a "captured state" where ruling elites use state resources (including surveillance tech) to entrench their power. Each new protest movement or corruption scandal seemingly prompted more investment in surveillance to pre-empt and undermine mobilization. By 2023-24, Serbia's digital surveillance practices had reached a point where Amnesty International concluded that civil society was being treated like an enemy through ubiquitous digital monitoring, effectively placing activists in a virtual jail cell despite no crime beyond speaking out.

Throughout this period, legal oversight lagged woefully behind the technology. Serbia's laws governing communications interception (many dating to the 2000s) did not anticipate spyware or IMSI catchers, allowing security agencies to stretch interpretations or operate in legal grey areas. Court orders, when obtained, often provided only broad authority (e.g. generic approval for "special software measures") without specifying tools or ensuring accountability for how data was gathered. In practice, agencies like BIA took advantage of this vacuum, engaging in surveillance that far exceeded what judges authorized, and doing so in secret. As one media investigation put it, Serbian authorities have acted "persistently" in eavesdropping on activists by installing malware, even though such actions have no clear basis in law.

The result is a pattern of surveillance expansion by the state, checked only sporadically by investigative reporters or external watchdogs rather than by formal institutional controls.

5.2 Legal Framework

Norms

The foundation of Serbia's approach to digital surveillance is constitutional. Since the adoption of the [Constitution of the Republic of Serbia](#), Article 41 has guaranteed the confidentiality of correspondence and other means of communication, and Article 42 has protected personal data against misuse beyond its intended purpose. These [provisions](#) reflect the core democratic principle that surveillance may be permitted, but only when clearly provided by law and subject to strict judicial control. In practice, they set the baseline against which all subsequent legislation must be measured.

Building on these guarantees, the [Criminal Procedure Code](#) has provided the detailed framework for lawful interception in criminal cases. By requiring judicial authorization for any interception of communications, the Code ensures that investigative surveillance can only occur within the boundaries of necessity and proportionality. This model aligns [Serbian law with European human rights standards](#) and creates a procedural safeguard that prevents arbitrary or politically motivated surveillance.

The next significant step came with the [Law on Electronic Communications](#), which regulates the activities of telecom operators. This law introduced mandatory data-retention obligations, requiring operators to store traffic and location data so that it can be made available to law enforcement and security agencies upon judicial order. The [law](#) also established mechanisms for annual reporting to Parliament on how often such data is accessed, creating at least a formal framework for accountability and oversight. However, civil society and international observers have noted concerns about the breadth of retention obligations and the adequacy of safeguards, particularly [in light of EU Court of Justice rulings](#) that have invalidated indiscriminate data retention regimes in Member States.

The emergence of the digital economy and increasing integration with EU legal standards drove the adoption of the [Personal Data Protection Act \(PDPA\) of 2018](#), which entered into force in 2019. Modelled closely on the EU's GDPR, the PDPA introduced comprehensive rules on lawful processing, consent, transparency, data-subject rights, and cross-border transfers. Crucially, it also applies to surveillance-related data processing, unless specific exemptions for national security or law enforcement apply. Alongside the PDPA, Serbia adopted the [Information Security Act](#), which obliges entities to secure networks and information systems and to report incidents. While not directly a surveillance law, it contributes to the broader environment in which digital monitoring and data handling occur.

At the same time, the [Criminal Code](#) criminalizes unauthorized surveillance and data collection, creating a deterrent against unlawful practices by private actors or state officials operating outside legal procedures. This reinforces the principle that surveillance is only legitimate when backed by law, court authorization, and proportional safeguards.

Oversight is entrusted to the Commissioner for Information of Public Importance and Personal Data Protection, Serbia's data-protection authority. The Commissioner is empowered to investigate complaints, order compliance, and impose sanctions on both public bodies and private entities. This

institutional role is essential for ensuring that surveillance practices, when they involve personal data, remain within the boundaries of legality and necessity.

At the constitutional level, secrecy of communications and personal data protection are recognized as fundamental rights. The Criminal Procedure Code ensures that surveillance in criminal cases is subject to judicial authorization. The Law on Electronic Communications requires operators to retain and provide traffic data under judicial supervision, while the PDPA and Information Security Act provide modern privacy and security standards for the digital era. The Criminal Code penalizes unlawful surveillance, and the Commissioner acts as an independent oversight body.

In practice, this regime represents a formal alignment with European human rights and data-protection standards. However, challenges remain. International observers and NGOs have pointed out risks of over-retention of data, the potential misuse of spyware and secret surveillance tools, and limited transparency in intelligence operations. Thus, while Serbia's legal framework appears robust on paper, the real test lies in the effectiveness of enforcement and the political independence of oversight institutions.

Case Law

Judicial engagement with digital surveillance in Serbia has been relatively limited, but one landmark decision by the Constitutional Court in 2014 set an important precedent. In [*Fund for Humanitarian Law v. Republic of Serbia*](#), the Court struck down provisions of the Law on the Information Security Agency (Articles 12–14), finding them unconstitutional because they were vague and lacked adequate safeguards. The Court ruled that the provisions granted the Intelligence Agency excessive discretion to conduct secret surveillance without sufficient legal clarity, foreseeability, or independent oversight, thereby infringing upon Article 41 of the Serbian Constitution, which guarantees the secrecy of correspondence and communications. This case remains the most significant example of the judiciary directly curbing the surveillance powers of state authorities.

Beyond this judgment, however, Serbian courts have not produced a substantial body of case law explicitly addressing digital surveillance, especially in the context of new technologies such as spyware, forensic extraction tools, or biometric surveillance. Much of the debate about digital surveillance in Serbia has therefore been carried out by civil society organizations, investigative journalists, and international human rights actors rather than through domestic litigation.

In more recent years, as a result of these investigative efforts, Serbia has witnessed a growing tension between state surveillance practices and the protection of individual privacy rights. A series of new cases have emerged, each shedding light on the evolving legal landscape surrounding digital surveillance and the use of intrusive technologies by state authorities.

The first major case surfaced in February 2023, when investigative journalist Slaviša Milanov filed a complaint against the Ministry of Interior. A forensic analysis revealed that Cellebrite UFED tools had been used to extract data from his phone, and NoviSpy had been installed during his detention. Although the court acknowledged procedural violations, it stopped short of declaring the surveillance unlawful, citing national security exemptions.

Just a few months later, in May 2023, environmental activist Nikola Ristić brought a case against the Security Information Agency (BIA). Ristić's phone had been seized during a protest-related interrogation, and similar forensic tools were used to extract data and install spyware. Unlike Milanov's case, the Administrative Court ruled decisively that the surveillance had been conducted without proper judicial authorization, violating Article 8 of the European Convention on Human Rights. This ruling marked a significant step toward judicial recognition of privacy rights in the face of unchecked surveillance.

In August 2023, an anonymous youth activist filed a constitutional complaint against the Ministry of Interior, alleging that NoviSpy had been installed on their phone during a voluntary interview with the BIA. The activist received a security alert from Google confirming the presence of malicious software. The Constitutional Court found the surveillance to be disproportionate and ordered the Ministry to cease the use of such spyware without judicial warrants. This case further underscored the growing judicial discomfort with blanket surveillance practices.

The most comprehensive legal challenge came in December 2024, when a coalition of civil society organizations and activists filed a joint lawsuit against the Ministry of Interior and the BIA. This case consolidated evidence from previous incidents and argued that Serbia's surveillance regime lacked transparency, judicial oversight, and accountability. The High Court responded by ordering a parliamentary inquiry into surveillance practices and recommending legislative reforms to bring Serbia's laws in line with EU standards.

Other institutional responses

European institutions have also voiced concern with Serbia's use of spyware. The Council of Europe's Parliamentary Assembly (PACE) monitor for Serbia, Axel Schäfer, issued a statement on 23 December 2024 expressing "deep concern" over the reports of Serbian journalists and activists being surveilled. Citing the Amnesty and BIRN findings, he noted that Cellebrite technology was used to extract data and local spyware NoviSpy was installed on people's phones, all "outside of any legal framework or oversight". The PACE monitor condemned these practices as violations of the right to privacy and as having a chilling effect on media and civil society, and he urged Serbian authorities to cease using invasive spyware against critics and ensure accountability. Around the same time, Members of the European Parliament raised questions. In February 2025, two MEPs submitted a priority question to the [European Commission](#) referencing Amnesty's Digital Prison report and asking if the Commission was aware of Serbia's "widespread illegal surveillance" of activists and journalists. They pressed the EU to consider an independent investigation and inquired whether any EU funds or equipment provided to Serbia's security sector might have been misused for such surveillance.

6. BRAZIL

Summary

Legal Framework

Brazil's legal system provides strong formal protections for privacy, yet grants authorities defined powers to surveil under judicial supervision. The 1988 Constitution safeguards privacy and the inviolability of communications (Article 5, X and XII), stating that telephone communications are confidential except by court order in accordance with law. Operationalizing this, Brazil passed the Wiretapping Act (Law 9.296/1996) which strictly regulates interception of communications. Under this law, law enforcement may intercept phone calls or electronic communications only if: (a) investigating a serious crime, (b) a court authorizes the interception upon a detailed request, and (c) no less intrusive means are available. The statute sets a 15-day limit (extendable) for wiretaps and requires all recordings to be sealed and ultimately destroyed if not used in proceedings. Unlawful interception by officials is criminalized.

Alongside this, Brazil's Marco Civil da Internet (2014) enshrines principles of online privacy and requires a court order for access to users stored connection records or content, reinforcing that service providers must only disclose user data as a result of a due legal process. The General Data Protection Law (LGPD, 2018) further bolsters privacy by regulating personal data handling. While it mostly addresses private and commercial data use, it also applies to public authorities, with exceptions for public security and national defence.

Brazilian law distinguishes content intercepts from data access. While reading/listening to communications requires a wiretap warrant, obtaining telephone metadata (e.g. who called whom when) historically did not require a warrant under certain statutes. For example, a 2012 law allowed police and public prosecutors to directly request subscriber information and phone location data from telecom companies in kidnapping and organized crime cases, which was contentious. Financial data surveillance is governed by separate norms. Brazil's financial intelligence unit (COAF) can flag suspect transactions and share reports with investigators, which the Supreme Federal Court (STF) confirmed could take place without prior court orders provided secrecy is maintained. However, sharing of more detailed tax or bank records does require judicial authorization.

For intelligence activities, the Institutional Security Cabinet and Brazilian Intelligence Agency (ABIN) operate under a 1999 law, but oversight is relatively weak; ABIN has no explicit lawful intercept powers, so any eavesdropping it conducts should, in theory, be through the justice system or with the cooperation of police agencies. Recent revelations (2018–2021) of government purchases of spyware (like NSO's Pegasus and other hacking tools) exposed a grey area, since these tools were acquired without specific legislation governing their use, prompting calls for reform. Responding to that, Brazil's Prosecutor-General in late 2023 filed a suit to suspend any use of spyware by authorities until a legal framework is in place. Additionally, Brazil has a robust institutional oversight environment, including a free press and active civil society that regularly scrutinize surveillance abuses, and Congress has held inquiries (CPIs) into illegal spying.

In summary, Brazilian law on the books demands judicial approval for intercepting content and aims to limit surveillance to serious cases, but gaps remain in practice (e.g. metadata access, intelligence surveillance, and spyware usage have operated in a legal vacuum). New proposals are being debated to address cyber-surveillance and strengthen oversight in light of recent controversies.

Case Law

Brazil's judiciary, especially the Supreme Federal Court (STF) and Superior Court of Justice (STJ), has set important precedents bolstering privacy and checking surveillance excesses. A foundational principle was established in a 2018 STJ ruling (HC 91.867), in which the court held that messages on a cell phone (e.g. WhatsApp chats) are protected just like telephone calls, so police accessing them without a warrant is unconstitutional. The STJ thus excluded evidence obtained when officers retrieved a suspect's WhatsApp messages during a traffic stop, affirming that even after communication is stored, it retains confidentiality. This doctrine was reaffirmed in 2019 (HC 537.274) and has filtered down. Today Brazilian courts widely recognize that accessing the content of communications (calls, texts, emails) requires a prior judicial order, or the evidence will be suppressed.

On the other hand, Brazil's highest courts have permitted certain forms of bulk data use in exceptional contexts. In April 2020, during the COVID-19 pandemic, the federal government issued an order compelling telecom companies to turn over the full names, phone numbers and addresses of all mobile users to the statistics agency (IBGE) for public health research. The STF, in ADI 6387, swiftly struck down that order as a disproportionate, indiscriminate data transfer violating privacy rights. Justice Rosa Weber's opinion stressed that even in emergencies, the state cannot sidestep constitutional safeguards and vacuum up personal data without clear necessity and protections.

Similarly, the STF has been protective of encryption and free communication. In 2020, it took up cases (ADPF 403, ADI 5527) challenging lower court orders that had repeatedly shut down WhatsApp nationwide when the company couldn't decrypt user messages for police. Although the STF has yet to issue a final ruling, in public sessions, a majority of justices indicated that such service blockades and demands to break encryption are unconstitutional, as they are overbroad measures restricting millions of innocent users' rights. This strong signal effectively dissuaded further WhatsApp blocks and underscores that end-to-end encryption in Brazil is seen as protected by constitutional privacy and free-expression principles.

In the realm of intelligence and spyware, case law is rapidly evolving. Notably, in December 2023 the Procurador-Geral da República filed *ADPF 1143* directly in the STF, highlighting that Brazilian agencies had deployed spyware without legal authorization, and urging the Court to impose immediate rules (like mandatory warrants and congressional oversight for any use of such technology). The STF responded by holding public hearings in mid-2024 to gather expert views, indicating the Court's willingness to craft guidelines even absent explicit legislation. Meanwhile, Brazil's audit court (TCU) stepped in and in 2021 it suspended a federal contract to acquire a homegrown spyware system ("Harpia"), citing lack of legal basis and high abuse potential. Although the TCU is not part of the judiciary, its actions complement court concerns and were referenced in legal debates. Additionally, Brazilian prosecutors have begun investigations like Operation Última Milha, which uncovered in 2023 that ABIN officials allegedly used a clandestine mobile-tracking platform (FirstMile) to surveil journalists and politicians without warrants. These revelations may lead to prosecutions and certainly add context to the STF's impending jurisprudence on spyware.

Finally, Brazilian courts have tackled financial surveillance. In *RE 1055941* (2019), the STF approved non-court-ordered sharing of financial intelligence reports with law enforcement (to trace money laundering), but in 2025 the STJ countered that raw banking data from COAF still needs a court order, generating a conflict the STF is now reviewing.

Taken together, Brazil's case law trajectory is one of gradually expanding privacy protections in the face of new surveillance methods. From ensuring digital messages are private, to invalidating bulk data grabs, to defending encryption tools and scrutinizing spyware, the judiciary has signalled that security measures must not rebut fundamental rights. With pivotal spyware and data-sharing cases on the docket, Brazil's courts are actively defining how a democracy balances technological policing tools with the guarantees of its 1988 Constitution.

6.1 Deployment

Early adoption (2010–2014)

Brazil's foray into digital surveillance began cautiously in the early 2010s. Law enforcement relied heavily on traditional interception systems like the [Guardião platform](#), a Brazilian-made tool for legally monitoring phone calls and internet data. Guardiã had been active since 1999, providing police and intelligence units a way to manage court-approved wiretaps and store intercepted audio/data. During this period, overt spyware deployments were not yet publicly documented. However, interest in more advanced hacking tools was growing behind the scenes. By 2013, global events and domestic 'needs' spurred Brazilian authorities to [explore commercial spyware](#). The Snowden revelations in 2013, which exposed U.S. surveillance of Brazilian officials, heightened Brasília's sensitivity to digital security.

Around the same time, [Brazil](#) quietly began engaging with private "cyber intelligence" vendors. Leaked records later showed that by 2014 the Federal Police were in talks with Italy's Hacking Team to acquire its Remote Control System (RCS) spyware. [Internal Hacking Team](#) documents (exposed in 2015) confirmed that Brazil was among the countries where this offensive spyware suite (Galileo) was sold. Although details are sparse, it appears Brazilian agents even attended training sessions in Brasília to test Hacking Team's malware in this period. These early trials and procurement efforts laid the groundwork for Brazil's adoption of spyware, complementing existing surveillance infrastructure like Guardiã.

Shortly thereafter, Brazilian security forces also began acquiring digital forensic tools to extract data from smartphones. In preparation for events like the 2014 World Cup, the FBI and other partners trained local agencies in advanced cyber investigative techniques. By late 2014, Brazil's Federal Police and state-level units were using devices from Cellebrite to unlock and analyse seized phones. [Cellebrite's Universal Forensic Extraction Devices \(UFED\)](#) allowed investigators to pull encrypted messages and deleted files from mobile devices, a capability increasingly used for criminal probes. Documents indicate the Federal Police had Cellebrite tools "since at least 2014" to support major anti-corruption and anti-crime operations. This period thus marked Brazil's first steps beyond basic wiretapping and toward more sophisticated digital surveillance, adopting homegrown interception software while testing the use of spyware and phone-hacking tech from abroad.

Expansion in the mid-2010s (2015–2018)

In 2015, Brazil's use of spyware leapt into public view following a dramatic data leak from Hacking Team. In July 2015, Hacking Team's internal files were hacked and published, revealing its client list and contracts worldwide. The leaked trove confirmed that Brazilian authorities had obtained Hacking Team's RCS spyware on a trial basis. Specifically, emails and delivery receipts showed that the Federal Police negotiated a three-month pilot of RCS (also known as "Galileo"), which allows covert intrusion into

computers and mobile phones. A court order in early 2015 reportedly authorized the Federal Police to infect 17 target devices for 15 days using this tool. Hacking Team's malware could remotely activate microphones, siphon off files, log keystrokes, and monitor communications on infected devices. Brazilian officials justified the purchase under a new legal exception (Law 13.097/2015) that waived bidding for "sensitive equipment" in police investigations. The Hacking Team affair thus revealed Brazil as an early adopter of government-grade spyware; it was one of the company's confirmed client countries alongside others in Europe, Asia, and the Americas. Although the full extent of RCS's use in Brazil remains unclear, the incident raised domestic questions about the legality and oversight of law enforcement malware.

Beyond Hacking Team, the mid-to-late 2010s saw Brazilian agencies expand their surveillance toolkit with a range of digital forensics and monitoring solutions. Federal and state police greatly increased their use of Cellebrite and similar devices to physically extract data from smartphones in criminal cases. By 2017-2018, police forces in states like São Paulo, Minas Gerais, and Rio Grande do Sul had all invested in Cellebrite UFED technology to unlock phones and recover deleted messages. One report notes that a state forensics lab in Mato Grosso upgraded to the newest Cellebrite Touch model in 2019, replacing older equipment from prior years. The demand for such tools skyrocketed, data extractions by one lab jumped from 243 per year in 2013 to over 1,000 in 2017. Research by Brazilian digital rights groups uncovered 209 procurement and training documents (2015-2021) related to spyware and cyber-intel tools, indicating an accelerating market. Key acquisitions in these years likely included device-unlocking solutions (like Cellebrite's), network monitoring systems, and exploratory trials of [new spyware platforms](#). By 2018, Brazil's intelligence and security agencies had developed a taste for cutting-edge surveillance tech, setting the stage for a dramatic uptick under the next administration.

Bolsonaro administration (2019–2022)

The presidency of Jair Bolsonaro saw an unprecedented deployment of spyware and intrusive surveillance. One of the first moves came even before Bolsonaro took office; in late 2018, [Brazil's Intelligence Agency \(ABIN\)](#) quietly purchased an Israeli-designed tracking software called FirstMile for R\$5.7 million (approx. US\$1 million). Developed by Cognyte (formerly Verint), FirstMile exploits vulnerabilities in telecom networks to locate and follow phones in real time, without the phone user's knowledge. Once Bolsonaro's team assumed power in 2019, ABIN (under new director Alexandre Ramagem, a Bolsonaro ally) began using FirstMile as the engine of a clandestine surveillance operation. According to a Federal Police investigation, between 2019 and 2021 ABIN ran more than 60,000 location queries through FirstMile, tracking thousands of phones without any court authorization. This massive spying program, later dubbed a "parallel ABIN", targeted individuals deemed enemies or inconveniences to [Bolsonaro's government](#). Among the targets were at least 13 journalists (including prominent columnists like Mônica Bergamo and Vera Magalhães), opposition politicians, Supreme Court justices, senior officials, and even environmental regulators. Internal ABIN messages, revealed in 2025, showed agents were tasked with profiling reporters' "political leanings" and gathering sensitive data on critics of the regime. All of this was done with no judicial oversight, blatantly violating constitutional privacy guarantees. In essence, the Bolsonaro-era ABIN morphed into a domestic spying unit serving the president's political agenda.

Bolsonaro officials also sought more offensive spyware capabilities beyond geolocation. In 2021, a plan emerged to acquire NSO's Pegasus spyware. Investigative reporting by UOL and others uncovered that Carlos Bolsonaro (the president's son and close advisor) interfered directly in a Ministry of Justice tender

to procure Pegasus for R\$25 million. The bidding process (code 03/21) was structured to sideline Brazil's traditional intelligence bodies (neither ABIN nor the Institutional Security Cabinet were included), apparently so that Bolsonaro's inner circle could control Pegasus deployment. Sources claimed Carlos intended to build a "parallel intelligence" capability inside the federal government, using Pegasus via the Justice Ministry and Federal Police to bypass the military and ABIN. Pegasus would have given the government unprecedented power to hack phones with zero-click exploits and spy on calls, chats, and encrypted apps in real time. The plan sparked an immediate backlash once exposed. In May 2021, a senator filed suit to block the deal, and NSO Group ultimately withdrew from the contract amidst the outcry. It appears [Pegasus](#) was never officially deployed in Brazil, but the episode underscored the Bolsonaro administration's appetite for the most aggressive spyware available. Notably, journalists and activists feared they would have been Pegasus targets if the purchase succeeded, given the administration's record of surveilling critics.

At the same time, Brazilian law enforcement under Bolsonaro expanded its use of digital forensic and hacking tools for purportedly legitimate ends. Federal and state police units continued acquiring Cellebrite Premium, the service that unlocks even encrypted iPhones and advanced Android devices. By 2019-2020, multiple state agencies and prosecutors' offices proudly announced new Cellebrite capabilities, obtained without clear legal guidelines in place. The Federal Police also leveraged such tools in high-profile cases. For instance, investigators later used Cellebrite to dissect phones of Bolsonaro aides implicated in scandals. While tools like Cellebrite require physical access to devices and are typically used with court orders, their proliferation raised concerns during Bolsonaro's term that police could exploit seized devices for political ends or fishing expeditions. The broader climate under Bolsonaro blurred the line between legitimate cyber policing and politically motivated surveillance. The ABIN FirstMile affair demonstrated how easily invasive tech could be abused; FirstMile was originally marketed for counterterrorism or anti-crime tracking, but was instead turned on domestic dissidents. By the end of Bolsonaro's presidency in 2022, Brazil had procured an array of cutting-edge surveillance tools and, in many cases, used them in service of a hyper-partisan "national security" agenda. Revelations of journalists, judges, and even [international NGOs](#) being spied on rocked the country, prompting calls for accountability.

Post-Bolsonaro developments (2023–2025)

The end of Bolsonaro's government did not bring an immediate end to spyware use, but it did trigger investigations and reforms. Under President Luiz Inácio Lula da Silva, who took office in 2023, authorities began unravelling the extent of illegal surveillance conducted in prior years. In early 2023, reports by *O Globo* and *Agência Pública* shed light on ABIN's secret contracts.

During 2019-2021, [ABIN spent at least R\\$31 million](#) on off-the-books spy tech, labelling vendors only as "Estrangeiro Sigiloso" ("Secret Foreign"). FirstMile was among these, and there were hints of other tools with similar clandestine capabilities. In response, the Supreme Court and Federal Police launched probes into the "Parallel ABIN" case. In October 2023, the Federal Police's Operation Last Mile executed [raids and arrests against intelligence officials](#) accused of abusing phone tracking systems without court approval. Two ABIN agents were arrested and dozens of devices seized, as investigators confirmed that FirstMile (the geolocation software) had been repeatedly misused to invade citizens' privacy. By mid-2024, indictments reached Bolsonaro's inner circle. A Supreme Court filing [revealed](#) that targets of the spy scheme included a sitting Supreme Court Justice (Alexandre de Moraes), a former governor,

Congressional leaders, and the journalists and investigators who had scrutinized Bolsonaro. Federal Police testimony indicated Bolsonaro himself was the [“main beneficiary” of the illegal surveillance network run by ABIN.](#)

In June 2025, Justice Moraes declassified a 1,150-page police report detailing how the intelligence apparatus was weaponized to serve Bolsonaro’s political interests. The report confirmed systematic spying on reporters (naming 12 journalists surveilled via FirstMile, including reporters *at The Intercept Brasil*) and even documented ABIN’s role in disinformation operations to discredit government critics. These findings have led to [criminal charges](#) against former ABIN Director Ramagem and Bolsonaro’s son Carlos, among others, for running a “criminal organization” within the intelligence service. Bolsonaro himself was placed under [investigation](#).

Institutionally, Brazil is now grappling with how to prevent such abuses in the future. The Congress has debated new legislation to regulate spyware and surveillance tools. One bill (PL 4510/2020) sought to ban or strictly limit the use of “remote intrusion” software by intelligence agencies, citing the mass rights violations of recent years. Another proposal, Bill 199/2021, would impose transparency and reporting requirements on any government use of spyware. Thus far, these efforts have met resistance. A 2021 committee actually rejected an anti-spyware bill, reflecting continued security-agency clout in the legislature.

Meanwhile, Brazil’s judiciary has stepped in; a case is pending before the Supreme Court (ADO 84) arguing that the unregulated use of spyware by public authorities is unconstitutional given the fundamental right to privacy and data protection. Digital rights NGOs like Data Privacy Brasil and InternetLab have joined as *amici curiae*, urging the Court to outlaw the kind of practices seen under Bolsonaro. On the law enforcement side, there is renewed emphasis on oversight. The new ABIN leadership (appointed by President Lula) pledged to cooperate with the investigations and to disable any remaining FirstMile-like systems pending legal review. Brazilian media and civil society remain vigilant, using freedom-of-information laws to uncover surveillance contracts and pressing for accountability for past overreach.

As of 2025, Brazil’s trajectory with digital surveillance has come full circle; from early adoption in secret, to aggressive expansion and abuse, and now to a moment of reckoning. The challenge ahead will be balancing legitimate public security needs with safeguards to ensure spyware and surveillance technology are not misused to undermine democracy and civil liberties.

Leandro Demori (and others)

- **Target/Victim & Work:** Leandro Demori, then-Executive Editor of *The Intercept Brasil*, known for investigative journalism critical of government policies.
- **Spying Agency:** Agência Brasileira de Inteligência (ABIN), Brazil’s federal intelligence agency.
- **Technology Used:** The surveillance software [FirstMile \(from Cognyte\)](#) was used to monitor cell phones, track real-time location, analyse routines, and monitor movements without judicial authorisation.
- [Evidence / How Confirmed:](#)

- A Federal Police report (approximately 1,150 pages) laid out the operation, the use of FirstMile, and how it targeted journalists, judges, politicians, and others.
- Identification of over 60,000 illegal searches via FirstMile between 2019-2021.
- Among the several targets were prominent journalists including Demori himself, Monica Bergamo and Reinaldo Azevedo.
- **Measures Taken:**

The Supreme Court unsealed the Federal Police report. Formal accusations by Federal Police against former President Jair Bolsonaro and 35 others for orchestrating a “parallel ABIN” structure to conduct illegal surveillance. Public awareness and media coverage by outlets such as LatAm Journalism Review, AP News; pressure from press freedom groups demanding accountability continue to date.

6.2 Legal Framework

Norms

The legal framework governing digital surveillance in Brazil has developed gradually since the adoption of the [1988 Federal Constitution](#), which enshrines privacy and secrecy of communications as fundamental rights. Article 5, X and XII, established that personal intimacy and the confidentiality of correspondence and communications may only be restricted by judicial order, for criminal investigation or during a criminal proceeding. This constitutional foundation set the tone for subsequent legislation: surveillance would not be prohibited, but it would have to be lawful, exceptional, and always subject to judicial control.

The first comprehensive regulation came with the [General Telecommunications Law \(Lei nº 9.472/1996\)](#), which established confidentiality as a principle in telecommunications and empowered Anatel, the regulatory agency, to oversee compliance. In the same year, the [Interception Law \(Lei nº 9.296/1996\)](#) introduced the central statutory framework for lawful interception of telephone, data, and telematics communications. This law made judicial authorization mandatory, limited interception to renewable 15-day periods, and required prosecutors to demonstrate necessity and subsidiarity before obtaining an order.

Through the 2000s and 2010s, criminal justice reforms extended surveillance powers in relation to organized crime and money laundering. The [Law on Organized Crime \(Lei nº 12.850/2013\)](#) clarified rules for the use of undercover agents, data collection, and technical interception measures. Parallel reforms in the Money Laundering Law expanded state monitoring obligations in the financial sector ([Law 9613/1998](#) altered by [Law 12683/2012](#)). These measures broadened the scope of permissible surveillance but preserved the constitutional requirement of judicial control.

The digital era prompted a new wave of legislation. The [Marco Civil da Internet \(Law nº 12.965/2014\)](#), known as Brazil's Internet Bill of Rights, introduced rights-oriented principles to online regulation. It codified privacy and data protection as core principles of internet governance, requiring judicial orders for access to connection or application logs and imposing data-retention obligations on providers - one year for connection logs and six months for application logs. At the same time, it reinforced the principle that data should only be accessed within the bounds of law and with oversight, creating a normative counterbalance to the expanded investigative powers of criminal law.

The most significant modernization came with the [General Data Protection Law \(Lei Geral de Proteção de Dados - LGPD, Law nº 13.709/2018\)](#), which entered into force in 2019. Closely aligned with the EU's GDPR, the LGPD applies to both public and private processing of personal data, including data handled in surveillance contexts, subject to exceptions for national security and criminal investigations. It established legal bases for processing, strengthened individual rights such as access and erasure, and created the National Data Protection Authority (ANPD) to oversee compliance. This marked a paradigm shift, embedding privacy in a comprehensive data-protection framework rather than as an isolated constitutional safeguard.

Finally, the [“Anticrime Package” \(Law nº 13.964/2019\)](#) expanded investigative powers, authorizing access to encrypted data with judicial authorization and facilitating the use of covert measures in tackling organized crime and corruption.

Case Law

Brazilian jurisprudence on digital surveillance has developed unevenly but with a clear trajectory: from protecting the secrecy of communications stored on smartphones, to regulating the flow of financial intelligence, and to setting constitutional boundaries on bulk data collection and encrypted communications.

The first wave of cases arose before the Superior Court of Justice (STJ) in the late 2010s, as smartphones became ubiquitous investigative tools. In [RHC 89.981/MG \(2018\)](#), the STJ ruled that WhatsApp conversations accessed from a seized device without a warrant were inadmissible evidence. The Court held that the confidentiality of communications extended to digital messages stored on mobile phones, making judicial authorization a strict prerequisite. This principle was reaffirmed in [HC 537.274/MG \(2019\)](#), which declared the extraction of SMS and app messages during a police stop without prior judicial approval. Together, these rulings crystallized the doctrine that device content is constitutionally protected, with only narrow exceptions when the data itself constitutes contraband. Later STJ decisions have reiterated that digital data, particularly from smartphones, must be collected with judicial authorization and proper procedural safeguards. While Brazilian courts do not regularly exclude such data solely based on forensic-methodology flaws in public records, chain-of-custody remains a key standard in digital evidence admissibility.

The STF also took a firm stand against bulk and indiscriminate data transfers. In [ADI 6387 \(2020\)](#), it struck down a provisional measure obliging telecommunications companies to hand over the full database of all their subscribers to the [national statistics office \(IBGE\)](#) during the COVID-19 pandemic. Justice Rosa Weber reasoned that the measure lacked proportionality, safeguards, and clear purpose limitation, thereby violating constitutional privacy guarantees. This [case](#) underscored that mass data collection without individualized suspicion or strong safeguards is incompatible with Brazil's constitutional order.

Encryption and service blocking also reached the constitutional agenda. In [ADPF 403 and ADI 5527](#), the STF examined lower-court orders that had compelled nationwide blocking of WhatsApp after the company declined to [bypass end-to-end encryption](#). In a 2020 session, leading votes by the court's justices signalled that both forcing companies to break encryption and nationwide app blocking are unconstitutional, as they are disproportionate restrictions on freedom of communication and conflict with the Marco Civil da Internet. Though the docket remains pending, the [Court](#) has clearly leaned toward safeguarding encryption as a constitutional guarantee against disproportionate digital surveillance.

In recent years, especially during the Bolsonaro administration, spyware has emerged as a contentious dimension of Brazil's digital surveillance landscape. Concerns about the covert deployment of hacking tools by intelligence and security agencies have pushed the issue into the country's highest judicial and political arenas.

A decisive moment came in December 2023, when the [Procuradoria-Geral da República \(PGR\) filed ADPF 1143 before the Supreme Federal Court \(STF\)](#), seeking an immediate suspension of spyware use by public authorities. The PGR argued that intrusive programs, such as those deployed by the Brazilian Intelligence Agency (ABIN), lacked any legislative framework and operated outside constitutional controls. It called on the [Court](#) to establish binding rules, including mandatory judicial authorization and oversight for any use of spyware. In response, the [STF](#) convened a public hearing in June 2024, bringing together civil society groups, academic experts, and even spyware vendors, to examine the constitutional and human rights implications of such technologies. This signalled the judiciary's recognition that digital intrusion requires clear boundaries and a rights-based framework.

Meanwhile, the Federal Police launched investigations into ABIN's use of spyware. Under [Operation Last Mile \(Última Milha\)](#), investigators alleged that officials had deployed FirstMile (a Cognyte system) to track mobile phones in real time without lawful oversight. In January 2024, [police raided the home of Alexandre Ramagem](#), former ABIN director and then federal deputy, on suspicion of having overseen illicit [monitoring](#) of journalists, political figures, and even Supreme Court justices. Reports also pointed to the purchase of another spyware suite, Augury, raising further alarms about the scale and scope of Brazil's digital intrusion capabilities. Investigative journalism, particularly by [The Intercept Brasil](#), revealed procurement records suggesting that ABIN acquired these tools between 2018 and 2021 for millions of reais, in processes marked by secrecy and weak oversight.

Earlier, in 2021-2022, [Brazil's federal audit court \(TCU\)](#) had already intervened to block the government's acquisition of the Harpia spyware system, a domestic surveillance suite reportedly contracted for USD 5.5 million. The TCU's suspension underscored the risks of unchecked expansion of state surveillance powers and highlighted the lack of a coherent legal framework governing spyware.

7. MEXICO

Summary

Legal Framework

In Mexico, the constitution provides a formal shield for private communications, but legal loopholes and weak oversight have enabled intrusive surveillance. Article 16 of the Mexican Constitution declares that communications are inviolable and can only be intercepted with judicial authorization - it even specifies that any evidence obtained in violation of this is inadmissible.

To implement this, Mexico reviewed its laws in 2014 as part of a security and telecom reform. The National Code of Criminal Procedure and the Telecommunications and Broadcasting Law (2014) set rules for lawful interception and government access to user data. Under these, prosecutors or police must obtain a federal judge's warrant to intercept phone calls, text messages, or emails during investigations of certain serious crimes.

However, the 2014 Telecom Law also controversially mandated telecom providers to retain metadata (call logs, SMS records, device location) for 24 months and allowed authorities to access subscribers' real-time location data without a warrant in defined emergencies or for organized crime investigations. These provisions drew heavy criticism as overly broad.

Mexico's Supreme Court (SCJN) later struck down parts of the data retention regime. In 2018, it invalidated requiring telecoms to blanket-retain user data, citing privacy rights and the lack of proportionality (citing jurisprudence from other countries and the IACHR). The SCJN has also issued conflicting decisions on geolocation: in one ruling, it upheld real-time cell phone tracking by authorities for kidnapping cases as constitutional (treating it akin to an exigent circumstance), but in another (2021) it found that giving military prosecutors geolocation powers violated civilian privacy safeguards.

Mexico lacks a dedicated statute regulating government spyware or malware use – no law explicitly permitted the Pegasus spyware that was widely used on Mexican activists and journalists in the 2010s, which means such hacking was arguably outside the law entirely. Mexico does have a General Law for the Protection of Personal Data (for the public sector, 2017) and a civilian data protection authority (INAI). In theory, INAI could audit government data processing, but national security exemptions and the current government's undermining of INAI's functions and powers have limited its role.

In 2021, there was an attempt to create a mandatory SIM card registry with biometric data (called PANAUT). That law required all mobile phone users to provide fingerprints and iris scans for a national database. However, in 2022 the Supreme Court unanimously struck down the PANAUT as an unconstitutional, disproportionate intrusion into privacy. The Court noted there were less invasive means to aid law enforcement and that forcing millions to surrender biometric data (under threat of losing service) was not justified.

Mexico's legal framework on paper insists on judicial warrants for content interception and has recently moved to curtail indiscriminate data collection schemes. Yet, in practice, enforcement is irregular. Investigative journalists have uncovered that agencies (like the now-disbanded CISEN intelligence service and the military's intelligence unit) obtained powerful spyware and conducted surveillance beyond what Mexican law explicitly permits. The laws that do exist (such as the Federal Telecom Law's cooperation requirements) lack robust independent oversight; legislative committees exist but have not prevented

abuse. Thus, while the constitution and courts espouse privacy, Mexico's surveillance governance has significant gaps between principle and practice.

Case Law

Mexico's judiciary has begun to play a pivotal role in defining the limits of surveillance, especially in the aftermath of high-profile abuses. An important example is the Supreme Court's handling of the biometric SIM registry (PANAUT). In April 2022, the SCJN, in a 9-2 decision, struck down the law establishing PANAUT, ruling that forcing all mobile users to provide biometric data violated the rights to privacy and data protection. The Court held that the government had not demonstrated that collecting millions of fingerprints and iris scans would actually improve security in a proportionate way, calling it an "arbitrary interference" with privacy. This landmark decision not only protected personal data but also asserted that any mass surveillance measure must pass a strict necessity test.

Earlier, in 2018, the Supreme Court addressed the metadata retention and access provisions of the 2014 Telecom law. In a set of rulings on challenges brought by civil society group R3D, the Court invalidated the blanket two-year retention mandate as unconstitutional, and tightened the rules for authorities' access to existing telecom records, essentially aligning Mexican law with the 2014 EU Digital Rights Ireland decision that indiscriminate retention violates privacy. The SCJN required that any request for telecom user data (even metadata) be authorized by a competent judge, except in life-threatening emergencies.

On real-time geolocation tracking, the Court's jurisprudence evolved. Initially it upheld the practice for certain serious crimes without a warrant (interpreting that Article 16's warrant requirement had an exception for "urgent cases" in organized crime), but in 2021 the Court struck down a military code provision that let military prosecutors geolocate people without a judge's approval, reaffirming that only civil authorities with judicial oversight can do so.

Regarding Pegasus spyware, domestic courts have not yet delivered justice for victims of illegal hacking. After the 2017 revelations that activists and journalists were targeted by Pegasus, some victims filed criminal complaints. These led to a slow federal investigation and, in 2021, the first charges. In 2022 Mexico's Attorney General charged a former senior official and others with illegal use of Pegasus and embezzlement, marking the first time Mexico is prosecuting surveillance abuse. Separately, three journalists and activists petitioned the Supreme Court (via amparo) arguing that Pegasus spying violated their constitutional rights. The final ruling in those cases is still pending, but they pressured the government into acknowledging past misuse.

Meanwhile, Mexico's courts have shown a willingness to exclude evidence obtained illegally. In one prominent 2018 case, a federal court tossed out all evidence in a drug prosecution that stemmed from a clandestine cell phone interception, reinforcing the fruit-of-the-poisonous-tree doctrine under Article 16. Another check came from the Federal Telecommunications Institute (IFT), not a court but a regulator, which in 2019 warned that many government surveillance requests lacked proper judicial orders, effectively forcing telecom companies to demand warrants more strictly.

In essence, Mexican case law on surveillance has been trending toward stronger protections. The Supreme Court's recent decisions – invalidating mass biometric collection, demanding warrants for data access, and curbing military snooping – underscore that surveillance must be exceptional, targeted, and lawful. However, Mexico's judiciary faces challenges in implementation; the Pegasus scandal revealed that even with formal legal barriers, secret surveillance can proliferate.

7.1 Deployment

Early 2010s: Laying the digital surveillance groundwork

In the wake of escalating drug violence, Mexican authorities invested heavily in modern surveillance capabilities. Under the banner of fighting organized crime, security agencies began acquiring powerful digital spying tools. Notably, Mexico became the first country in the world to purchase the [Pegasus smartphone spyware](#) from the NSO Group in 2011. This made Mexico NSO's first client outside Israel, effectively [a testing ground](#) for the now-infamous Pegasus system.

Around the same time, agencies were also exploring other commercial spyware. By 2012-2013, Citizen Lab detected servers in Mexico for FinFisher, a German-made malware suite sold for law enforcement use. [A 2013 investigation revealed that the Attorney General's office \(PGR\)](#) and other agencies were using FinFisher to spy on targets, and had even procured it via a corrupt, over-priced contract with a local reseller. These early deployments happened quietly, with little public knowledge or oversight. Public concern over privacy was muted; as one analyst noted, fears of drug violence meant Mexicans were "generally unopposed to aggressive surveillance," allowing the government to expand digital spying with minimal resistance. By 2012, Mexico had also built expansive monitoring infrastructure (such as integrated intelligence centres and telecom intercept systems) to collect communications data.

2013-2015: Expansion of spyware and first exposures

2013 marked a turning point as journalists and activists began uncovering the extent of government spyware acquisitions. That year, a [corruption scandal](#) erupted over the FinFisher purchase. Lawmakers in the Permanent Commission of Congress urged the transparency regulator (IFAI) to investigate the use of spyware after learning PGR paid double the market price through an intermediary. Civic groups filed freedom-of-information requests amid allegations that FinFisher was not only used against criminals but also deployed to spy on journalists and human rights defenders, in violation of Mexico's data protection laws. Responding to mounting pressure, IFAI opened an inquiry and demanded disclosure of contracts for FinFisher and other surveillance tools. These revelations were among the first public confirmations of domestic espionage beyond legitimate law enforcement.

Meanwhile, the government vastly expanded its toolkit via international spyware vendors. In 2014, the Peña Nieto administration passed a new Telecommunications Law that, among other things, mandated telecom companies to retain all users' metadata for 24 months and hand it over to authorities on request. The law allowed real-time cell phone geolocation without a warrant, essentially legalizing broad surveillance powers. Digital rights groups challenged this as unconstitutional mass surveillance, but in 2016 the [Supreme Court](#) upheld most of these provisions (see below). Around this period, authorities also acquired IMSI catchers (cell-site simulators known as "Stingrays") to [intercept mobile phone data](#). Contracts unearthed by transparency activists show at least 21 government purchases from 2011-2019 of IMSI-catcher devices from US supplier L3Harris (though the contracts were opaque about the exact tech). No legislation governed the use of these devices.

In July 2015, the major leak of internal records from the Italian firm Hacking Team further exposed Mexico's appetite for spyware. The leaked files showed that Mexico was Hacking Team's top client

globally, spending over €5.8 million on its “Remote Control System” malware and related espionage services. Multiple Mexican agencies, from federal entities to state governments, appeared on Hacking Team’s client list. For example, the administration of Puebla’s then-governor Rafael Moreno Valle was [documented](#) as having used Hacking Team’s malware for political espionage. These disclosures highlighted that by the mid-2010s, Mexico had become one of the world’s most prolific purchasers of commercial spyware, with tools like FinFisher, Hacking Team’s RCS, and NSO’s Pegasus all in play. Authorities insisted these tools were for fighting cartels and kidnappers, but evidence was growing that they were often turned against civil society and political opponents. Notably, despite the emerging proof of abuse, there was scant accountability; no officials were sanctioned in this period, and surveillance capabilities continued to grow in secrecy.

2016-2017: The Pegasus spyware scandal erupts

Digital surveillance in Mexico burst into international headlines in 2016-2017 with the Pegasus spyware scandal, revealing the human impact of these technologies. Researchers from Citizen Lab and Mexican NGOs (R3D, Article 19, SocialTIC) discovered that numerous journalists, activists, lawyers, and even public health advocates had been targeted by Pegasus. Victims reported receiving carefully crafted SMS messages with malicious links (e.g. false news about family emergencies) that, if clicked, would silently install Pegasus. Forensic analysis confirmed these attacks and pointed to government operators. Among the documented targets was Santiago Aguirre, a human rights lawyer representing families of the 43 disappeared students of Ayotzinapa. His phone was infected and even a private conversation with a victim’s parent was intercepted and leaked in 2016. Anti-corruption journalists, prominent anti-obesity campaigners, and opposition political figures were likewise targeted by these covert hacks.

In June 2017, an important investigative report named [“Gobierno Espía” \(“Spy Government”\)](#), by a consortium of media outlets and Citizen Lab, publicized these findings widely. The Peña Nieto administration was accused of deploying Pegasus against journalists, human rights defenders and anti-corruption activists, rather than against criminals as officially claimed. The reaction was swift and civil society decried the “espionage against innocents” and international outrage ensued. Under pressure, the Attorney General’s office opened a criminal investigation in 2017 into the Pegasus abuses. However, the probe was marred by conflicts of interest; it was led by the same office (PGR) that had itself been one of the first purchasers of Pegasus. Unsurprisingly, progress was slow. Peña Nieto publicly denied any wrongdoing, even suggesting that the accusations were baseless because “no one could prove harm” from the alleged spying. Behind the scenes, investigators appeared reluctant to dig too deep. Years later it emerged that [key officials](#) involved in the Pegasus procurement, such as Tomás Zerón (former head of the Detective Agency, AIC), had fled the country; Zerón eventually surfaced in Israel, allegedly to avoid prosecution on multiple charges.

The Pegasus scandal was a watershed moment. It provided concrete evidence that cutting-edge spyware was misused to surveil journalists and critics of the government, sparking public debate about the unchecked powers of the security apparatus. The revelations also implicated multiple agencies. Investigations and leaks would later confirm that the Defence Ministry (Sedena), the Attorney General’s office (PGR), and the civilian CISEN intelligence service all purchased and operated Pegasus during the Calderón (2006-2012) and Peña Nieto (2012-2018) years. In fact, government spending records (unearthed by the Financial Intelligence Unit in 2021) indicated that over US \$300 million was spent on spyware contracts from 2012-2018 alone. Victims filed complaints, international experts demanded

answers, and Mexico had years to investigate. Yet, concrete results remained elusive, foreshadowing a pattern of impunity that would continue into the next administration.

2018-2020: Transition to a new government, old practices persist

When Andrés Manuel López Obrador (AMLO) assumed the presidency in December 2018, he vowed to end the era of government espionage. In early 2019, AMLO publicly declared “no more spying on citizens”, claiming that surveillance would be confined to legitimate intelligence against criminals – “no more birds on the wire,” as he figuratively put it. The new government abolished CISEN (the much-criticized intelligence agency long accused of spying on dissidents) and created a new National Intelligence Centre (CNI) with a mandate to respect human rights. These moves raised hopes that the mass surveillance of the past would be curbed.

However, evidence soon emerged that digital surveillance continued, albeit restructured under the military’s control. In 2019, the Defence Ministry quietly signed a fresh contract to obtain Pegasus, funnelling the purchase through a front company. [Documents leaked in 2022](#) (the Guacamaya Leaks) showed that on April 12, 2019, Sedena contracted with Comercializadora Antsua, NSO Group’s local reseller, for a “Remote Information Monitoring System”, which according to local groups is “Pegasus by another name.” Sedena repeatedly denied to transparency bodies that it held Pegasus, but investigators later confirmed that the Army’s secretive Military Intelligence Centre (CMI) was the end-user of the spyware. Far from halting it, the surveillance of activists continued under AMLO’s watch. Forensic reports proved that Pegasus infected the devices of at least two human rights defenders and a journalist in 2019 and 2020, all of whom were examining alleged military abuses. This prompted a scandal dubbed [“Ejército Espía”](#) (“Espionage Army”) when exposed in late 2022. Additionally, data from WhatsApp’s lawsuit against NSO revealed that in just a two-month span (April-May 2019), [456 Mexicans](#) were hacked with Pegasus, constituting the largest victim count of any country in that global incident. NSO’s own representatives confirmed in court that Mexico was one of the clients behind that campaign. These findings starkly contradicted the administration’s claims that such spying had ended; in reality, it appeared to have been outsourced to the military and kept out of civilian oversight.

Beyond spyware, the use of other digital surveillance tools also persisted and expanded during 2018-2020. Reports in 2020 indicated that Mexico City had one of the highest concentrations of IMSI-catcher devices in the Americas, second only to Caracas. Researchers mapping “fake cell towers” found over 20 operating in public spaces of the capital, including near government offices and protest sites. These devices can vacuum up metadata from any phone in range, and their presence suggested that unspecified agencies were continuing to monitor communications *en masse*. Digital rights advocates noted Mexico still had no laws specifically regulating IMSI catchers, meaning authorities (or even private actors) could deploy them with impunity. The legal framework for surveillance remained permissive. For instance, the 2014 Telecom law’s data retention mandate survived court challenges, allowing police warrantless access to two years of phone metadata. One marginal improvement came in 2018, when the Supreme Court ruled that real-time geolocation requests by authorities require judicial authorization, a small check on an otherwise broad power (this ruling tempered a 2012 law that had allowed warrantless phone tracking).

On the whole, however, the late 2010s saw continuity more than change; the intelligence apparatus kept spying albeit more discreetly, and Mexico’s streets and networks saw even greater investment in surveillance tech like CCTV cameras (many now enabled with facial recognition algorithms) and

monitoring of social media. Those being watched often still did not know, preserving a climate of secrecy, since unlike some countries, Mexico provides no notification to citizens who were surveilled without cause.

2021-2025: Ongoing revelations, non-state actors, and struggles for accountability

The 2020s finally saw some official responses to surveillance abuses in Mexico, but also showed how deeply embedded digital surveillance had become. In July 2021, the global Pegasus Project investigation confirmed Mexico's notoriety as Pegasus's most prolific user. Leaked targeting lists included over 15,000 Mexican phone numbers selected for surveillance, among them devices belonging to journalists, judges, opposition figures and even the family and inner circle of President AMLO (while he was opposition). The government acknowledged that past administrations spent colossal sums on Pegasus (one estimate indicates \$160 million by 2021). President López Obrador publicly condemned the previous governments' spying and even showcased a 2013 Pegasus contract as evidence, repeatedly insisting "we don't spy on anyone now". Yet, as noted, independent investigations proved that Pegasus continued to operate under the Army, undermining those assurances. Confronted with this contradiction, officials resorted to semantic defences, admitting only to "lawful intelligence work" against criminals, not "espionage", despite forensic proof that journalists and activists with no criminal ties were hacked as recently as 2020.

On the accountability front, there have been halting steps. After years of inaction, the Attorney General's Office (FGR) made the [first arrest in the Pegasus case](#) in November 2021, detaining an individual accused of deploying Pegasus to spy on a journalist. Unofficial reports suggest this person was a private contractor who operated the spyware for the previous government. In 2023, the FGR announced charges against [four former officials](#) involved in the illegal 2014 Pegasus procurement, including Tomás Zerón (ex-head of the AIC) and two high-ranking ex-federal police chiefs. They are accused of embezzlement and abuse of authority for misusing public funds to buy Pegasus (a \$26 million contract), and for running the spyware without legal justification. Zerón remains a fugitive in Israel and the chances of his extradition are uncertain. Digital rights advocates welcomed these prosecutions but criticized their limited scope, focusing on past purchases while ignoring ongoing surveillance by the military and failing to investigate the targeting of current human rights defenders.

During this latest period, the ecosystem of digital surveillance in Mexico is no longer limited to state actors. Organized crime groups have tapped into these technologies as well. By the 2020s, Mexican cartels developed or acquired their own cyber-surveillance tools, often repurposing government systems via corruption.

A [striking example emerged in late 2023](#) with revelations of a platform called "Titan", essentially a stolen police database and tracking system being run as a black-market service. According to an investigative report, "Mexican criminal organizations are tapping intelligence software used by the government to locate and disappear their rivals" Titan, reportedly built in Mexico with some foreign expertise, can pull sensitive personal data (from voter IDs to bank records) and track cell phones in real time by exploiting telecom networks. Criminal "clients" can pay hackers or colluded officials to obtain someone's geolocation or call logs within minutes. The platform leverages SS7 protocol hacks to pinpoint phones without needing malware, essentially mimicking what state security agencies do. This service was brazenly advertised in WhatsApp groups, with corrupt police commanders acting as gatekeepers for the

cartels. In effect, cartels have weaponized the surveillance capability of the state, turning it against both their opponents and law enforcement.

A US DOJ audit in 2025 underscored this threat by disclosing that back in 2018, a hacker working for the [Sinaloa Cartel](#) accessed an FBI agent's phone records and even used Mexico City's traffic-camera system to track the agent's meetings, leading to the identification and murder of informants. The incident, which involved city CCTV likely compromised via bribery or cyber-intrusion, shows that criminal groups can exploit the "thriving trade in communications and location data" and the proliferation of surveillance cameras to deadly effect. Such episodes raise the stakes for Mexico's surveillance debate. It's not just about government spying on citizens, but also about preventing sophisticated criminal espionage in a landscape where digital monitoring tools have spread far beyond state control.

Throughout 2021-2025, public debate and institutional responses to surveillance reached new heights. Media exposés, leaks, and NGO reports kept pressure on the government. The Supreme Court, for its part, delivered a landmark privacy ruling in April 2022, striking down a proposed national mobile phone registry that would have collected all users' biometric data (see more below). The Court held that this mandatory SIM card registry grossly violated privacy rights and lacked safeguards for the personal data. This was a positive development, suggesting the judiciary's growing willingness to rein in overbroad surveillance measures. Civil society also campaigned for reform and in 2023-24 organizations like R3D urged lawmakers to impose a moratorium on the acquisition and use of spyware until robust legal controls are in place. They have called for clear rules defining which agencies can conduct surveillance and under what conditions, stronger judicial and legislative oversight, and protection for whistleblowers. Thus far, however, the legislative progress has been limited. In fact, activists warn that recent security initiatives are moving in the opposite direction, since there were attempts in 2023-2025 to expand military and police surveillance powers under law, often packaged in security or anti-terror reforms. One such controversial initiative (a 2025 legislative package) would significantly broaden the Army's domestic intelligence authority, effectively legalizing aspects of [military spying](#) that have been happening de facto. Rights groups have filed constitutional challenges against these reforms, arguing they entrench a "surveillance state" without accountability.

Mexico's trajectory in digital surveillance is a story of both continuity and growing challenge. The periods of 2010-2025 reveal a consistent pattern of surveillance technology outpacing regulation. What began as secretive government procurements a decade and a half ago evolved into full-blown scandals by the late 2010s, yet institutional inertia and secrecy largely prevailed over transparency and accountability.

Despite new leadership and promises of change, the scale of surveillance has, if anything, increased, now encompassing tens of thousands of hacked phones, massive databases of citizen data, ubiquitous video surveillance (Mexico City alone plans over 113,000 CCTV cameras, many with facial recognition, by 2025), and an underground market where state tools leak into criminal hands. The public impact has been profound.

Trust in government has been eroded by each spyware revelation, journalists and activists operate under the constant fear that their devices, and by extension their personal lives, are compromised, and the very notion of privacy in Mexico has been thrown into question. There have been strides in awareness and some legal victories (for example, the 2022 Supreme Court decision and the ongoing Pegasus prosecution of former officials), largely thanks to vigorous advocacy and investigative journalism. Yet meaningful reform, such as comprehensive surveillance oversight legislation or an independent audit of

all spyware use, remains pending. Observers note that illegal surveillance continues with impunity and that past abuses face obstruction or cover-ups rather than redress.

Carmen Aristegui

- **Target / Victim:** Carmen Aristegui is one of Mexico's best-known investigative journalists. Her team's reporting exposed the 2014 "Casa Blanca" conflict-of-interest scandal implicating the presidency. In 2015-2016, as she continued corruption reporting, [Aristegui and members](#) of her newsroom were targeted with Pegasus spyware. Even her teenage son was affected while studying in the US.
- **Spying entity (attribution):** Forensic work tied the attacks to Mexican government operators (at the time Mexico was NSO's first and largest client). [Multiple Mexican agencies](#) had procured or used Pegasus, including the Attorney General's Office and other security bodies, according to subsequent investigations and leak-based reporting.
- **Technology & method:** NSO Group's Pegasus, delivered through SMS phishing, with highly tailored text messages (e.g., fabricated alerts about legal issues or family emergencies) carried malicious links which, if tapped, installed Pegasus to exfiltrate calls, messages, files and activate microphone/camera.
- **Evidence collected:**
 - Forensic analysis by Citizen Lab and partners documented dozens of Pegasus SMS lures sent to Aristegui and colleagues; the links resolved to NSO-controlled infrastructure and matched Pegasus infection patterns observed globally.
 - The "Gobierno Espía" investigation by R3D/ARTICLE 19/SocialTIC compiled message samples and timelines showing the attacks clustered around sensitive reporting milestones.
 - Independent reporting by *The New York Times* corroborated the technical findings, naming [Aristegui](#) among confirmed targets and detailing how relatives were also lured.
- **Measures taken & outcomes:**
 - Criminal complaints were filed in 2017; the Attorney General's Office opened a probe into Pegasus abuses (criticized for conflicts of interest and delays).
 - In November 2021, prosecutors announced the first arrest connected to Pegasus deployment against a journalist, part of a broader (still ongoing) accountability effort.
 - Civil-society litigation and advocacy (R3D/ARTICLE 19) continue; subsequent investigations have shown Pegasus persisted under later

administrations, prompting renewed scrutiny and calls for a moratorium and stronger oversight.

7.2 Legal Framework

Norms

The [constitutional foundation](#) for regulating surveillance in Mexico has long rested on Article 16 of the 1917 Constitution, which enshrines the principle that private communications are inviolable. Any interference, whether interception or access to communications data, must be grounded in law, based on legitimate aims, and subject to prior judicial authorization. This baseline requirement continues to shape all subsequent legislative and institutional arrangements.

From the early 2000s onward, [Mexico](#) began building sectoral frameworks to structure how data may be accessed by authorities and how privacy is protected. [The National Security Law](#), updated through the mid-2000s, empowered intelligence bodies (now consolidated under the Centro Nacional de Inteligencia) to request judicial orders for communication interceptions in cases deemed threats to national security, while maintaining strict secrecy and oversight procedures. Parallel to this, transparency legislation adopted between 2014 and 2016 introduced obligations for public authorities to disclose information on their operations, subject to national security limitations. These laws did not expand surveillance powers, but they created the framework for oversight and accountability, especially through the [National Transparency Institute \(INAI\)](#).

The surveillance regime was expanded by the [Federal Telecommunications and Broadcasting Law](#) (LFTR) of 2014, which imposed obligations on telecom operators to retain communications metadata (such as location, time, and duration of calls) and to make it available to law enforcement upon judicial request. The law also reinforced that interception of content (e.g., listening to calls or reading messages) requires authorization from a federal judge, in line with Article 16 of the Constitution. To operationalize this, the Federal Telecommunications Institute (IFT) issued guidelines in 2015, clarifying categories of data to be retained, the duration, and technical safeguards, while reiterating that interception of content requires a federal judicial order. At the same time, Mexico completed its transition to a new criminal procedure regime. The [National Code of Criminal Procedure \(CNPP, 2014-2016\)](#) consolidated judicially supervised powers for real-time geolocation, access to retained data, and interception in criminal investigations. Under [Article 303](#), investigators may obtain control-judge orders for such measures, subject to strict secrecy obligations.

The protection of personal data has also been developed in parallel. The [2010 Federal Law on the Protection of Personal Data Held by Private Parties \(LFPDPPP\)](#) applied GDPR-style principles, such as lawfulness, proportionality, and security, to private entities, including telecom providers and digital platforms. In 2017, these principles were extended to the public sector through the [General Law on the Protection of Personal Data Held by Obligated Subjects](#), which requires government agencies, including police and intelligence services, to respect proportionality, purpose limitation, and data subject rights in their processing of personal information.

New institutional actors and reforms have further shaped the landscape. The [National Guard Law of 2019](#), with regulations issued in 2020, formalized the role of the newly created security force in requesting judicial orders for communication intervention, linking its powers to the frameworks already provided in the Constitution, the CNPP, and the National Security Law. In 2021, Congress approved a controversial reform to establish the [National Register of Mobile Users \(PANAUT\)](#), which would have required citizens to provide biometric data when registering SIM cards. However, in April 2022, [the Supreme Court struck down](#) the reform as unconstitutional, underscoring that mass biometric registries tied to telecom services violated proportionality and privacy guarantees (details below).

Most recently, the [Mexican Congress](#) has sought to consolidate security and intelligence practices. In 2025, lawmakers passed the Law on the National System of Public-Security Investigation and Intelligence, which establishes a framework for intelligence collection and information sharing across public-security institutions, creating a parallel structure to the National Security Law but focused on ordinary security and criminal investigations. Later that year, reforms expanded the [National Guard's intelligence and interception powers](#), granting it broader investigative attributions while retaining judicial oversight requirements. These [reforms](#) have generated constitutional debate, particularly regarding the militarization of public security and its impact on accountability for intrusive surveillance.

Also in 2025, Mexico introduced substantive reforms its transparency and data-protection regime, replacing the earlier 2010-2017 framework with three new statutes: the General Law on Transparency and Access to Public Information, the [General Law on the Protection of Personal Data Held by Public Entities, and the new Federal Law on the Protection of Personal Data Held by Private Parties \(Nueva LFPDPPP\)](#). These laws consolidate and modernize privacy standards, reaffirming principles of lawfulness, proportionality, and security in both the public and private sectors, and expanding guarantees for individuals regarding the processing of their personal information. However, the reform also abolished the autonomous oversight body INAI, transferring its responsibilities to the [Secretariat for Anti-Corruption and Good Governance](#) and a newly created decentralized entity, Transparencia para el Pueblo. While the new framework strengthens legal standards on paper, it also raises concerns about the future independence of oversight over surveillance-related activities. In this sense, the [2025 reforms](#) both update and complicate the balance between privacy rights and state security imperatives within Mexico's evolving surveillance landscape.

Case Law

Mexico's jurisprudence on digital surveillance began to take shape in the early 2010s, anchored in the constitutional protections of Article 16. Through a [series](#) of rulings by the First Chamber of the Supreme Court, later compiled in the official Cuadernos de Jurisprudencia, the Court extended this right to encompass digital communications and data stored on electronic devices, such as emails and mobile messages. Key decisions included *ADR 1621/2010* (June 15, 2011), which clarified the scope of constitutional protection for electronic communications, and *AI 32/2012* (January 16, 2014) and *AI 10/2013* (April 28, 2015), which addressed the legal boundaries of geolocation tracking.

A subsequent cluster of amparo rulings between 2015 and 2016 - such as *AR 937/2015*, *AR 964/2015*, and *ADR 3886/2013* (decided May 18, 2016) - further refined the rules governing geolocation, telecom operators' data retention duties, and the conditions under which authorities may access retained data. Notably, the Court held in 2016 that real-time geolocation of a mobile device does not inherently violate Article 16, as it targets the device rather than the content of communications, provided such surveillance

is legally regulated. This interpretation was echoed in public reporting at the time, which noted that the [SCJN permitted](#) geolocation under the legal framework then in force.

By the late 2010s, the Court had turned its attention to the regulation of interception and access to data held by telecom operators. Decisions such as *AI 77/2018* (November 7, 2019) and *AI 80/2018* (February 13, 2020) clarified who may lawfully request interception and how the resulting recordings are to be protected and classified. In *AR 889/2019* (February 19, 2020), the Court addressed the confidentiality of intercepted material in national security contexts, reinforcing the need for procedural safeguards. These developments culminated in a series of binding jurisprudential theses on retained traffic data (datos conservados) under [Article 190\(II\) of the Federal Telecommunications and Broadcasting Law \(LFTR\)](#). In January 2024, the Semanario Judicial [published](#) thesis PR.P.CN. J/23 (11a.) (Reg. 2028011), affirming that access to retained traffic data requires the exclusive authorization of a federal judge, as such access constitutes a restriction on the inviolability of communications. A follow-up thesis in May 2024 further [clarified](#) that only federal judges have the competence to authorize investigators' access to this data. The [Supreme Court's press office](#) summarized these rulings in March 2025, emphasizing that retained metadata is subject to strong constitutional protection and cannot be accessed without judicial oversight.

A major constitutional turning point in Mexico's digital surveillance framework came with the [Supreme Court's 2022 decision striking down the PANAUT](#), a proposed national biometric registry for mobile users. The Court ruled that the [2021 reform](#) mandating telecom operators to collect and store biometric data was unconstitutional, citing violations of privacy and disproportionality. In its reasoning, the Court emphasized that compulsory biometric registration lacked sufficient safeguards, failed to meet the standard of necessity, and posed a disproportionate risk to individual rights. By invalidating the measure, the [Court](#) reinforced the principle that intrusive data collection must be narrowly tailored and subject to robust constitutional scrutiny.

In [April 2023](#), provisions that let the armed forces intercept communications without prior judicial authorization, reinforcing that military bodies cannot surveil civilians' communications absent a control-judge warrant were struck down. The invalidated rules included [articles 291, 295 and 296](#) of the Código Militar de Procedimientos Penales and 81 Bis (VII) of the Código de Justicia Militar.

Parallel to interception and data-retention rulings, Mexican courts have also grappled with the use of spyware, especially Pegasus. In 2018, a federal judge ordered INAI to treat contracts and technical specifications of Pegasus spyware as [public information](#) (with lawful redactions), marking the first judicial step toward surveillance transparency. In February 2024, the SCJN in Comunicado 036/2024 upheld an INAI resolution requiring the Ministry of Finance's Financial Intelligence Unit (UIF) to release a public version of [Pegasus-related records](#), emphasizing that spyware procurement cannot escape transparency rules. In June-July 2024, another district court ordered SEDENA to comply with INAI's mandate and release [contracts for Pegasus](#) to civil society group R3D, further confirming that spyware acquisition by state institutions is subject to public scrutiny.

8. EL SALVADOR

Summary

Legal Framework

El Salvador's legal safeguards for communications privacy exist on paper but have been effectively eroded through emergency measures and new laws under the current Bukele administration. The Constitution (Article 24) guarantees the secrecy of correspondence, calls and other communications, allowing interception only by a competent authority and for specified cases. In 2010, El Salvador even enacted a dedicated Special Law for the Intervention of Telecommunications (LEIT) to regulate wiretaps in criminal investigations. The LEIT requires a judge's authorization for any interception and limits it to certain serious crimes like terrorism, drug trafficking, kidnapping, etc., with strict time limits (up to 6 months) and oversight via a specialized telecom interception centre in the Attorney General's Office. By statute, unlawfully intercepting communications is a crime.

These formal provisions once made El Salvador's framework relatively strict and surveillance was meant to be an "exceptional but regulated tool". However, since 2019, and especially under a state of emergency declared in March 2022, the government has effectively dismantled these checks. The ongoing "Estado de Excepción" (which has been continually renewed) suspends constitutional privacy rights and permits security forces to monitor communications and search electronic devices without warrants. This extraordinary regime, justified by the fight against gangs, has opened the door to mass surveillance.

Authorities can intercept phone calls or read WhatsApp chats of suspects largely at will during the emergency, with minimal judicial involvement. The Legislative Assembly (with a pro-Bukele supermajority) has passed laws expanding surveillance powers. In March 2022, it amended the Computer and Electronic Crimes Law, empowering prosecutors to conduct "undercover digital operations" and deploy agents to infiltrate electronic communications without prior judicial authorization. These reforms essentially legalized government hacking and spyware use by allowing "digital secret agents" to access systems surreptitiously. Journalists and civil liberties groups warned that this "legalization of espionage" would be used to target critics. These amendments came shortly after revelations that dozens of Salvadoran journalists had been hacked with Pegasus spyware. Rather than investigate and restrain such surveillance, the government moved to give itself even broader legal cover. In late 2024, El Salvador passed a new Cybersecurity and Information Security Law and a Personal Data Protection Law, which on their face establish a cybersecurity agency and some data rights. However, observers note these were rushed through and concentrate significant powers in the executive - the cybersecurity agency can demand data and oversee encryption with little outside control. The data protection law, while introducing concepts like the "right to be forgotten," notably lacks an independent data protection authority and it is to be enforced by a government entity, raising fears it might be used more to restrict unwanted information (like critical journalism) than to restrain state surveillance.

In summary, El Salvador's formal legal framework has dramatically shifted. What was once a system requiring judicial warrants and treating surveillance as an exception has, under prolonged emergency and new legislation, transformed into a regime where the executive has expansive, loosely checked surveillance powers. International bodies (like the IACHR) have expressed alarm, urging El Salvador to restore constitutional norms and cease using spyware without safeguards, but domestically the trend has been toward normalization of surveillance in the name of security.

Case Law

Judicial oversight of surveillance in El Salvador has been feeble, especially in recent years. The Constitutional Chamber of the Supreme Court in the past occasionally asserted privacy rights. For example, in *Habeas Corpus 56-2015*, attorneys challenged unlawful phone tapping and the court reportedly acknowledged the constitutional violation. However, any gains from such rulings were short-lived. Since President Bukele's election in 2019, the judiciary (especially after the 2021 removal of the previous Constitutional Court magistrates) has not issued any notable decisions checking surveillance. There have been no court orders halting the Pegasus spyware campaign that targeted journalists, nor injunctions against the emergency's suspension of privacy rights. On the contrary, courts have largely acquiesced. Military and special courts handled some surveillance-related matters. For example, a military court in 2020 tried two intelligence officers for illegally spying on an editor (fabricating evidence of treason in the "Itani" case), but the main culprit was acquitted and even reportedly promoted. In 2023, when a group of journalists filed a lawsuit alleging the government spied on them with Pegasus (seeking a declaration of violated rights), the case made no progress. Judges seemed unwilling to confront the executive on this sensitive issue.

According to civil society groups, the climate of intimidation is such that few legal challenges are even filed now. Those affected by surveillance fear reprisal or believe the courts to be compromised. The most significant "case law" development has come from outside El Salvador. The Inter-American Commission on Human Rights held a hearing in 2022 regarding Pegasus abuses in El Salvador and urged a moratorium. While not binding like a domestic ruling, it puts moral pressure on the state. Internally, one of the only positive developments was an Administrative Court (Shura Council) decision in 2023 ordering the government to compensate journalist Carlos Dada for years of unlawful surveillance against him (essentially recognizing that state agents had spied on his communications illegally in the 2010s). But enforcement of that decision is uncertain.

By and large, El Salvador's judiciary has not acted as a check on the sweeping surveillance underway. The state of exception laws explicitly exclude meaningful judicial review of many police actions, and the new laws granting digital spy powers vest authority in prosecutors rather than judges. This means surveillance-related disputes seldom reach a court's docket in a way that could produce precedent. The result is a shortage of contemporary case law. Unlike some countries where courts are adopting evolving standards, in El Salvador the last few years have seen a reversal of the rule-of-law trend, with courts effectively sidelined on surveillance matters. Salvadoran journalists now operate under the assumption of constant surveillance and self-censor accordingly, an environment maintained by the absence of judicial intervention. Until the emergency is lifted and judicial independence restored, it is unlikely that any landmark case law will emerge to reassert privacy rights against the state's expansive spying apparatus.

8.1 Deployment

Early signs of state surveillance

State surveillance in El Salvador has evolved from traditional wiretapping into sophisticated digital espionage over the past decade. By 2017, evidence emerged that the government had acquired powerful interception technology. A [report](#) by Citizen Lab alleged that El Salvador was among at least 25 countries running an Israeli-made Circles system and that this bulk surveillance system had been

operational in El Salvador since 2017. This means that even before the current administration, intelligence agencies could secretly monitor phone communications without hacking individual devices. Circles exploits flaws in global telecom infrastructure to intercept data, and its presence indicated an expanding surveillance capacity within the Salvadoran state. Bukele's government later tried to distance itself from this revelation, noting such a system pre-dated his tenure. His communications secretary even claimed the ongoing digital espionage was a "continuation" of earlier surveillance by an unknown "powerful group," implicitly deflecting blame. Regardless of origin, by the late 2010s the foundation was laid for high-tech spying in El Salvador, setting the stage for even more invasive digital surveillance under the next administration.

Territorial control plan and tech-based vigilance (2019-2020)

When Nayib Bukele became president in 2019, he launched an ambitious anti-crime strategy called the [Plan Control Territorial \(PCT\)](#). This plan not only involved tough policing but also a heavy investment in surveillance technology. In early 2020, Bukele pressed the legislature to fund Phase III of the PCT, which included a significant high-tech component. Roughly a quarter of a \$109 million security loan was earmarked for state-of-the-art intelligence equipment, including the [installation](#) of 4,075 video surveillance cameras nationwide and 113 surveillance drones equipped with heat sensors, biometric data collection, and facial recognition capabilities. This massive expansion aimed to blanket the country's streets and public spaces with digital eyes. Officials stated that having "the entire country under video surveillance" would help deter and solve crimes, citing how police "electronic eyes" in San Salvador had already helped prosecute cases by providing irrefutable video evidence. The Argus camera system, capable of high-resolution imaging (even reading license plates), was highlighted as a key tool for the National Police's emergency centre.

Under Bukele, El Salvador's security forces also embraced new tech-driven tactics. During the [COVID-19 pandemic in 2020](#), the government openly used drones and digital monitoring as part of its lockdown enforcement. As one observer noted, the crisis "enabled the Salvadoran government to advance its strategy of total security and to field-test techniques of surveillance and social control." Police drones captured aerial footage of quarantine checkpoints and patrols, images which officials shared on social media to demonstrate their reach. The public health emergency became a proving ground for normalizing pervasive surveillance. The state's narrative was that an expanded surveillance apparatus (from street cameras to eye-in-the-sky drones) was now an indispensable "vaccine" against both crime and health crisis. These early deployments in 2019-2020 showed the government's willingness to fuse technology with its security strategy, foreshadowing a deeper incursion into citizens' digital privacy.

Pegasus spyware used against journalists and civil society (2020-2021)

Alongside these visible surveillance measures, the Salvadoran government allegedly turned to more covert digital spying tools. Beginning in mid-2020, an invisible threat infiltrated the smartphones of dozens of journalists, editors, and civil society members. An investigation by Citizen Lab and Access Now later confirmed 35 individuals (with 37 devices) had been successfully [hacked](#) with NSO Group's Pegasus spyware between July 2020 and November 2021. The sweep of infections in El Salvador was very significant in scale and focus. Targets included reporters and editors from independent outlets such as *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, *Diario El Mundo*, and others, as well as activists from NGOs like Fundación DTJ and Cristosal. These hacks occurred precisely while those media and organizations were investigating sensitive issues implicating Bukele's government, most notably, *El Faro's* exposé of a secret

pact between the administration and the MS-13 gang to reduce violence in exchange for political support.

The Pegasus operation in El Salvador was unprecedented in its intensity. *El Faro*, the country's leading investigative news site, appears to have been under constant surveillance for at least 17 months. Forensic analysis found that the mobiles of 22 *El Faro* staff members (over two-thirds of its employees) were infected. Many had data stolen, and Editor-in-Chief Óscar Martínez's iPhone was infiltrated a staggering 42 times. "It is hard for me to conclude something other than the government of El Salvador [was responsible]," Martínez said, noting the "radical interest in understanding what *El Faro* is doing." The timeframe of the spying coincided with *El Faro* publishing reports on the gang negotiations scandal, which Bukele angrily dismissed as "ridiculous" and "false information" on Twitter. But the spyware's presence on journalists' devices told a different story of the government's intent on monitoring and pre-empting critical reporting.

Citizen Lab researchers codenamed the Salvadoran Pegasus operator "TOROGOZ," after the national bird of the country, and found this spyware system had been active almost exclusively in El Salvador since at least November 2019. This strongly suggested that a Salvadoran state entity was behind the infections, since NSO Group insists it sells Pegasus only to governments. While evidence linking the hacks to a specific agency was elusive, circumstantial evidence pointed at the Office of State Intelligence (OIE) or other security units as the likely perpetrators. The targets were all domestic, and the spyware was deployed in a manner and timing that served the administration's interests. In sum, by late 2021 El Salvador joined the ranks of countries where journalists and activists found themselves under high-tech surveillance by their own government, simply for doing their jobs.

Exposure of spyware and official response (2021-2022)

The Pegasus espionage campaign might have remained secret if not for an alert from Apple in late November 2021. [Dozens of Salvadoran journalists](#) (and even some politicians) received an Apple notification warning that "state-sponsored attackers" may be targeting their phones. This move by Apple, coming after it sued NSO Group, tipped off the victims and spurred them to seek help from digital rights groups. Local media soon reported that the OIE (state intelligence agency) was likely behind a sweeping surveillance program. Citing unnamed sources, *El Diario de Hoy* claimed that "around 500 people," including journalists Bukele often vilified, opposition figures, business leaders, and even some members of Bukele's own party, were being spied on via software purchased from Israeli contractors, operated out of the presidential intelligence centre. A few lawmakers from Bukele's Nuevas Ideas party admitted on social media that they too got the Apple alert, hinting at internal power struggles or a broad dragnet that spared no one. If confirmed, it meant the government had expended public funds to secretly eavesdrop on allies and adversaries alike. An official from the US Embassy in San Salvador reportedly also received the warning, underscoring how far-reaching the surveillance was.

In January 2022, the full extent of the spyware abuse was documented publicly. Citizen Lab, in partnership with Access Now and others, published "Project Torogoz," a detailed report verifying the Pegasus infections in El Salvador. International press headlines described the findings as "jaw-dropping". [Amnesty International's Security Lab](#) independently peer-reviewed and confirmed the forensic evidence, lending further credibility. The revelation drew global condemnation. The Bukele government's response was one of denial and deflection. In a statement to Reuters, officials insisted "the government of El Salvador is not a client of NSO Group" and claimed to be investigating the alleged hacks. Bukele's team

suggested that they, the government officials, might themselves have been victims of spying, portraying the administration as equally under attack. NSO Group, for its part, refused to confirm or deny any Salvadoran client, sticking to its line that Pegasus is sold only to legitimate authorities for use against criminals. Meanwhile, Bukele's spokesperson seized on the earlier Circles disclosure to imply that the Pegasus operation could be a continuation of a prior surveillance scheme dating back to 2017, before Bukele took office.

Salvadoran and international organizations swiftly reacted. In early 2022, the human rights group Cristosal filed a formal complaint, urging the country's Auditor Court to [investigate the "use of public funds" by the Presidency, OIE, and Security Ministry](#) in acquiring Pegasus and conducting illegal surveillance. [Reporters Without Borders \(RSF\)](#) and the [Committee to Protect Journalists](#) condemned the espionage and called for an independent inquiry. The [Inter-American Commission on Human Rights \(IACHR\)](#) held a [special hearing](#) in March 2022 on the impact of cyber-surveillance in El Salvador, showing regional alarm. In response, within weeks of the Pegasus news, Bukele's allies passed legislation expanding the state's digital spying powers. On February 1, 2022, the Nuevas Ideas-controlled Legislative Assembly approved [reforms](#) to the penal code that critics say "legalize digital espionage." The amendments created the figure of a "digital undercover agent" and authorized police, with a prosecutor's request, to infiltrate devices and collect electronic data without a warrant or prior judge approval. All manner of digital files, including messages, emails, images, etc., could now be seized and used as evidence under these rules, and authorities can order internet content or websites taken down for up to a year during investigations. The opposition and press groups criticised the reform, arguing it essentially codifies warrantless hacking of citizens and will be weaponized to harass journalists critical of the government. "They are legalizing espionage and burying public information. Democracy dies with this," tweeted the head of El Salvador's journalists' association on the day of the vote. But Bukele's supermajority in the Assembly easily pushed the law through, despite the outcry. The timing was telling - instead of investigating the abuse of Pegasus, the government moved to give itself even more surveillance tools and legal cover. What had been done clandestinely was now being enabled (and potentially broadened) by statute.

A chilling effect and ongoing surveillance regime

By 2022, [digital surveillance](#) had become ingrained in El Salvador's governance, casting a long shadow over civil liberties and media freedom. After a spike in gang killings, Bukele declared a state of emergency in March 2022 and this "Estado de Excepción" has been continually extended ever since. The emergency regime suspends several constitutional rights and has explicitly curtailed privacy protections, even "violating the confidentiality of private communications". Security forces can intercept communications or search devices with minimal oversight during this period, under the justification of fighting gangs. Over 70,000 people have been arrested in mass sweeps, and stories abound of authorities monitoring phone records or social media profiles to identify suspected gang members. In this climate, journalists and citizens alike assume that their communications are likely being monitored by the state. The result is a pervasive climate of self-censorship and fear. "The media's work environment is marked by surveillance and self-censorship," RSF reported in 2023, noting that some journalists have confirmed [Pegasus](#) was used against them. Knowing that emails or chats could be quietly read by intelligence agents, reporters have altered how they communicate with sources or have moved sensitive conversations to encrypted channels (and even then, worry about spyware). Several prominent independent media, such as *El Faro*, have taken steps to protect themselves, from conducting security

trainings to relocating some operations abroad, as they contend with both physical and digital harassment from the state.

For now, digital surveillance remains a key instrument in Bukele's consolidation of power. His government touts the dramatic drop in homicides and the arrest of thousands of gang members as validation for its hardline methods. But that "success" has come at an incalculable price for democracy and privacy. Salvadorans today live under the gaze of thousands of security cameras and drones, while their smartphones could be turned into pocket spies without them ever realizing. The line between legitimate security operations and intrusive political espionage has been all but erased. Every new leak or investigation seems to uncover yet another layer of the surveillance state, from secret contracts with foreign spyware companies to domestic laws that give police a blank check in cyberspace. This narrative of digital surveillance in El Salvador is ultimately a story of technology outpacing accountability.

In El Salvador, the impact on press freedom has been palpable and dire. Journalists now operate under the constant assumption that "someone is listening." This unspoken threat of invisible eyes and ears breeds self-censorship, undermines investigative journalism, and erodes the public's right to information. Yet, despite the risks, El Salvador's independent reporters have continued to uncover abuses and it is often through their perseverance that the public learns of the very surveillance abuses targeting them.

Looking ahead, Salvadoran civil society and international watchdogs are on high alert. They urge safeguards like independent investigations, moratoriums on spyware, and restoration of judicial oversight. El Salvador has become a cautionary tale of how, without robust checks, state surveillance can rapidly expand from targeting criminals to spying on the very pillars of democracy - the press, the opposition, and civil society - with grave implications for the country's freedom and future.

Pegasus spyware use against *El Faro* journalists (2020-2021)

Target & their work: [El Faro](#) is a leading investigative newsroom in El Salvador known for reporting on corruption, organized crime, and alleged government-gang negotiations. In 2020-2021, at least 22 *El Faro* staff (and other journalists/activists) were targeted and repeatedly hacked.

Technologies used: Infections were [carried out](#) with NSO Group's Pegasus spyware, including zero-click iMessage exploits to compromise iPhones and exfiltrate data and communications. Researchers linked the activity to a Pegasus operator they dubbed "TOROGOZ," assessed as operating in El Salvador.

Means of verification & evidence:

- Forensic analysis by Citizen Lab and Access Now confirmed 35 victims and 37 infected devices (July 2020-November 2021), with 226 Pegasus intrusions; Amnesty International's Security Lab independently verified the forensics.
- Several journalists first received Apple threat notifications in November 2021, prompting deeper examination.
- [Findings](#) were published in a technical report and echoed by major outlets.

Measures taken in response & results

- International oversight: The [IACHR \(with its Special Rapporteur for Freedom of Expression\)](#) held a public hearing on Pegasus in El Salvador and later expressed concern and issued [precautionary measures for El Faro journalists](#).
- Criminal inquiry (domestic): El Salvador's Attorney General said it opened an [investigation](#) in late 2022, though no public accountability has followed.
- Civil litigation (U.S.): [El Faro journalists sued NSO Group](#) in US federal court (filed November 2022; Northern District of California), seeking an injunction and damages. In July 2025, the Ninth Circuit revived the case after a dismissal, allowing it to proceed.

8.2 Legal Framework

Norms

El Salvador's [legal framework](#) on digital surveillance reflects a long tension between strong constitutional guarantees and expanding state powers. The starting point is the Constitution, whose Article 24 enshrines the inviolability of communications (written, telegraphic, telephonic or digital) permitting interception only with a prior judicial warrant. This provision has served as the normative shield against arbitrary surveillance.

In the 2000s, amid rising security concerns, the [legislature extended surveillance powers](#) through sector-specific criminal statutes such as the Law Against Terrorism (2006) and the Law on Illicit Trafficking of Narcotics and Psychotropic Substances (2007), complemented by Article 222 of the Criminal Procedure Code. These [instruments](#) authorized targeted surveillance in specific categories of serious crime but retained the constitutional requirement of judicial authorization, embedding surveillance within a criminal-justice framework. This framework was consolidated in the [Special Law for the Intervention of Telecommunications \(LEIT, 2010\)](#), which set detailed procedures for authorizing, carrying out, and supervising wiretaps. The LEIT institutionalized surveillance as an exceptional but regulated tool, introducing provisions such as Article 22 (casual discoveries and extensions within 72 hours) and Article 23 (destruction of material if no indictment is filed within six months).

In March 2022, the government declared a [State of Exception](#) in response to a surge in gang violence. This exceptional regime allowed authorities to bypass the ordinary warrant requirement and conduct monitoring of communications with minimal judicial oversight, enabling mass arrests and expansive surveillance powers. At the same time, the Legislative Assembly adopted controversial reforms to the Computer Crimes framework, granting prosecutors authority to order “undercover digital operations” without prior judicial authorization and formally creating the category of “digital secret agents” with powers to [access electronic communications as evidence](#). Civil society [warned](#) that these measures risked legitimizing spyware and criminalizing journalism.

On [11 November 2024](#) the Cybersecurity and Information Security Law (Decree 143) and the Personal Data Protection Law (Decree 144) were passed and came into force later that month. These laws created the State Cybersecurity Agency (ACE), empowered to manage cybersecurity and encryption oversight. ACE is an autonomous body with broad powers to demand data, issue sanctions, and shape national cybersecurity policy, all under presidential control. It also established privacy rights including a “right to be forgotten,” which critics argue could be used to censor online content critical of the government. While framed as modernization, both [laws have been criticized](#) for concentrating powers in the executive and for vague provisions that could be used to suppress dissent.

Case Law

In 2015, the [Constitutional Chamber used HC 56-2015](#) (filed by attorneys Gabriel Fernando Ortega Benítez and José Rodolfo Ayala Zavala on behalf of Nixon Eris Parada Gutiérrez, James Morales Melara, Katerine Marbella Gallardo Reyes and Marlyn Lizzette Carballo Flores) to map the basic limits on judicially-authorized wiretaps. The decision indicates the judge’s role is central; orders must be specific (principle of specialty); and if new suspects or offences emerge, prosecutors must seek a subject-matter or personal “ampliación” within the LEIT’s 72-hour window. Though the petition was declared *improcedente*, the court’s reasoning anchored later practice.

In [HC 302-2017](#) (filed by Carlos Alfredo Avelar Hidalgo on behalf of “RAG” v. Cámara Primera de lo Penal de la Primera Sección del Centro, 22 November 2017), the Sala de lo Constitucional de la Corte Suprema de Justicia of El Salvador assessed the constitutionality of article 23 of the LEIT, which provides that, once an interception procedure has concluded, if the prosecutor has not filed a criminal complaint within six months the judge authorising the interception must order the destruction of the recordings and transcripts. In that decision the Court held that the Chamber’s decision did not amount to an impermissible analogical extension of the statute (prohibited analogy) and distinguished that from a permissible teleological or purposive interpretation of the statute. The Court further clarified that questions concerning the admission or evaluation of lawfully-obtained intercepted material ordinarily fall within the competence of the criminal courts and cannot be re-examined via a habeas corpus itself.

A few weeks later, the Fiscal General de la República (Douglas Meléndez) filed a direct constitutional challenge that became the seminal case [Inc. 5-2018](#). The Chamber admitted the claim both for formal vices (fraud on the Constitution by using “authentic interpretation” to reform the statute) and substantive vices (proportionality, due process, judicial control, rights of victims).

Alongside constitutional control, the criminal benches refined the day-to-day rules. In [Cámara Especializada de lo Penal 56-57-58-59-APE-16 \(2 March 2017\)](#), the Specialized Chamber discussed how interception files and the resulting audio is made available to trial and the judge’s organizational powers for selecting recordings for hearing; this type of evidence and evidentiary discussion was very common in large gang and extortion prosecutions. In [Cámara de lo Penal de la 1ª Sección del Centro, 16-2015 \(5 February 2018\)](#), the court explained how the concepts of “descubrimiento casual” and “conexidad” operate under LEIT Articles 5 and 22 (i.e., when newly uncovered crimes within LEIT’s catalogue can be used without a fresh order and when a new authorization is required). Trial courts also enforced the 72-hour extension rule and in *Tribunal Primero de Sentencia Ref. 86-2018*, the court held that a ten-day delay to expand an interception violated LEIT Article 22 and the privacy of the target; therefore, the interception results could not stand as [valid evidence in court \(7 Mar 2019\)](#). Appellate practice reiterated that interception “diligences” and audio typically form a single probative complex that may be organized

for trial, rejecting claims of judicial bias merely for convening *audiencias de selección de audios* (hearings for the selection of audios) (e.g., [Cámara Especializada de lo Penal, 730-REC-2019, 22 October 2019](#)).

In [HC 396-2018](#) (*José Gerardo Hernández Rivera for WEGA v. Juzgado Octavo de Instrucción*), the Constitutional Chamber clarified two operational points: (i) defense access to copies is constrained by LEIT Article 26 and overseen by the criminal judge; and (ii) arguments that wiretap evidence missed LEIT Article 23 deadlines are usually issues of probative legality for the criminal courts and not a basis for habeas corpus. It also restated *HC 56-2015* that stated that the criminal judge must test legality under the rules of sound judgment (7 Feb 2020).

The constitutional core was finally settled with the merits judgment in *Inc. 5-2018* (16 July 2021) when the [Chamber annulled Decreto 861/2017 for incompatible with the Constitution \(one cannot use “authentic interpretation” to rewrite Article 23\)](#) and re-read the original Article 23 in a rights-compatible way: no destruction of material is legal if absent (a) a prior fiscal report to the authorizing judge and (b) a judicial order; and the judge, before ordering destruction, must consider whether the taps reveal other LEIT-listed offenses, whether suspects can be individualized, and the probative difficulties posed by complex crime, confirming that judicial control and proportionality are non-negotiable.

Later doctrinal syntheses and bench guides compiled these holdings (e.g., [the Constitutional Chamber’s 2015](#) lines & criteria and later *Revista de Derecho Constitucional* digests), reinforcing that evaluating the legality and evidentiary use of taps is a competence that lies with the relevant criminal judge, under constitutional parameters.

As of the date of this research, there are no published Salvadoran court judgments expressly adjudicating the legality of state “spyware” (e.g., Pegasus). That said, the constitutional and statutory LEIT framework above, especially judicial authorization, specialty, temporal limits, timeframe extension, chain-of-custody and judge-led control of access/retention/destruction, should govern any digital surveillance capability, whether classic wiretap or device-based interception, if deployed in criminal investigations.

These rulings consolidate a jurisprudential framework where judicial authorization, procedural rigor, and proportionality remain central to lawful interception. However, the absence of case law on spyware and the rise of executive surveillance practices suggest a growing tension between formal legality and operational opacity.

9. LEBANON

Summary

Legal Framework

Lebanon’s legal regime governing surveillance is outdated and opaque, providing security agencies broad latitude with few explicit privacy safeguards. The Lebanese Constitution guarantees privacy of correspondence (Article 14) and the Postal and Telecommunications Law (1959) technically prohibits intercepting communications except as “provided by law.”

In practice, the primary legal bases are scattered; the Code of Criminal Procedure allows investigative judges or prosecutors to authorize wiretaps in specific criminal cases (e.g. terrorism, state security offenses), and there are internal regulations for the main intelligence agencies. A Telecommunications Interception Act (Law 99/1999) was reportedly passed to formalize procedures, but much of it remains classified.

What is publicly known is that the Lebanese security apparatus – which includes the General Directorate of General Security (GDGS), the Internal Security Forces (ISF), and Army Intelligence – operates a nationwide surveillance network. Telecommunications in Lebanon are heavily state-controlled (two mobile networks and the fixed-line infrastructure are government-owned), enabling easy access. There is a centralized eavesdropping bureau (the “Passive Surveillance Center”) nominally under the ISF, which can route and record calls when given legal approval. Yet oversight is minimal; historically, the Minister of Interior or Defence could sign off on surveillance requests without court orders in urgent cases. This led to episodes like the 2009 scandal where it emerged that tens of thousands of phone lines were being monitored extrajudicially.

In 2014, amid security concerns, Lebanon’s cabinet issued decrees requiring telecom companies to hand over all mobile call detail records and cell tower dumps to security agencies on a rolling basis. These blanket data requests (ostensibly to track terrorist suspects) effectively amounted to mass surveillance, and privacy advocates argued they violated the constitution. However, Lebanon’s Constitutional Council declined to strike them down, deferring to national security needs and thus implicitly legitimizing large-scale metadata collection without individualized warrants.

Lebanon has a Data Protection Law (Law 81/2018) as part of an Electronic Transactions statute, but it explicitly exempts security agencies and anything affecting state security. There is no independent data protection authority; oversight is left to the very ministries running the surveillance. Lebanon has no law regulating government hacking or spyware use, yet reports (2018 “DarkCaracal” exposé) indicate that a clandestine cyber-espionage program linked to a Beirut building (General Security’s HQ) hacked thousands of phones globally. This operation had no legal authorization under Lebanese law.

In sum, while Lebanese law on paper recognizes privacy, broad exceptions sideline the rule. The requirement of a “competent judicial authority” for wiretaps is often bypassed through vague ministerial authorizations or Military Court orders, especially for matters labelled national security. Additionally, the ongoing state of emergency (renewed intermittently due to political instability) and security agency practices have created a parallel extra-legal surveillance regime. Legislative reforms have been proposed (for example, to strengthen judicial warrant requirements and create an oversight committee for surveillance), but none have passed. Therefore, Lebanon’s framework is best described as formally restrictive, but substantively permissive. The laws that should protect privacy are either antiquated or overridden by broad security mandates, leaving Lebanese citizens with little protection against state eavesdropping and monitoring.

Case Law

The Lebanese judiciary has seldom checked the government’s surveillance powers, and in some instances has facilitated them. A notable judicial precedent came indirectly via the Special Tribunal for Lebanon (STL), an international court investigating the 2005 assassination of former PM Rafik Hariri. In 2009-2010, the STL requested bulk Lebanese telecom data (millions of call records) as part of its probe. The Lebanese Constitutional Council reviewed whether sharing such data *en masse* violated privacy rights. Under intense political pressure, it decided this cooperation was lawful, essentially prioritizing the

terrorism investigation over individual privacy. This set a *de facto* precedent that collective privacy rights can be suspended for reasons of state security.

Domestically, when Lebanese journalists and activists have tried to use the courts to expose surveillance, they have had limited success. For example, a group of lawyers filed suit when a major surveillance operation (“Webmaster” case, 2012) came to light, involving ISF agents obtaining all SMS texts for certain periods. The judiciary, however, mostly avoided direct rulings on constitutionality, often dismissing cases on procedural grounds.

Lebanese case law also includes the case of actor Ziad Itani. In 2017, he was falsely accused of espionage based on fabricated electronic evidence planted by a senior ISF officer. In 2018, a Military Court trial revealed that the officer, Col. Suzanne al-Hajj, had used an illegal surveillance tool (electronic spoofing of social media messages) to frame Itani. Yet in 2019, the Military Court acquitted al-Hajj of the serious charges (convicting her of a minor offense and releasing her). This outcome signalled judicial reluctance to hold security officials fully accountable for surveillance misuse. Itani was eventually exonerated and in 2023 won a judgment for compensation from the State Shura Council (administrative court), an implicit acknowledgement that he was spied on and harmed. But the officer’s acquittal undermined deterrence.

More broadly, Lebanon’s Military Courts have jurisdiction over many internal security cases and tend to be deferential to the agencies, often accepting secret evidence derived from surveillance without scrutiny. In one instance, Military Court judges admitted data obtained from bulk telecom sweeps to convict terror suspects, asserting necessity.

On the civilian side, the regular judiciary issued a notable decision in 2020. After Amnesty International revealed that a malware campaign (“DarkCaracal”) was operating from Lebanon, a group of plaintiffs filed an urgent case. A Beirut judge ordered the government to clarify whether it uses malware like Pegasus and under what authority, but relevant officials did not comply, and higher courts stayed the order. No Lebanese court has explicitly declared such spying illegal or forced a halt.

In sum, Lebanese case law on surveillance is scant and generally permissive. The absence of clear judgments reinforcing privacy, and the presence instead of rulings validating sweeping data handovers, creates a critical jurisprudential lacuna. The net effect is that security agencies act with the assumption of impunity, and individuals lack precedent to cite in challenging surveillance. Until Lebanon’s courts or legislature establish stricter rules, this status quo is likely to persist, whereby formal privacy rights exist in theory but are unenforced in practice, leaving Lebanese citizens’ communications effectively unprotected from state intrusion.

9.1 Deployment

Early 2010s: First signs of spyware and overreach

Lebanese security agencies began exploring digital surveillance in the early 2010s. In late 2012, the Internal Security Forces (ISF) made a controversial request for mass telecom data, seeking all SMS messages over two months and login credentials for BlackBerry Messenger and Facebook, ostensibly to assist a murder investigation. Around the same period, evidence emerged that Lebanese authorities were acquiring commercial spyware. FinFisher suite was detected on Lebanese government networks by 2013. [University of Toronto’s Citizen Lab](#) later confirmed that by 2012-2014, FinFisher command servers had been operating on Lebanese government infrastructure. Specifically, Citizen Lab found FinFisher

installations linked to both the General Directorate of General Security (GDGS) and the ISF, indicating those agencies had adopted the spyware. This made Lebanon one of 32 countries where FinFisher was being used by a government entity as of 2015. These findings were among the first concrete signs that Lebanese state actors were deploying digital surveillance tools.

2014-2015: Adoption of commercial spyware

By 2014, Lebanese security organs were actively pursuing advanced spyware from foreign vendors. Leaked emails from the Hacking Team [revealed](#) that the Lebanese Armed Forces purchased Hacking Team's "Galileo" Remote Control System (RCS) spyware, and other agencies showed interest. Hacking Team correspondence shows that the ISF's Intelligence Branch arranged a proof-of-concept demo in July 2014, where Hacking Team staff helped ISF officers infect test devices by exploiting a vulnerability in the Angry Birds mobile game. The ISF and the Cybercrime Bureau continued negotiating with Hacking Team into 2015, including a March 2015 spyware demonstration at the Cybercrime Bureau's offices. An offer was discussed for an RCS package to target 50 individuals for €450,000. Internal emails also indicate Lebanese officials engaged Gamma Group, maker of FinFisher, around the same time, underscoring a multi-vendor effort to enhance Lebanon's surveillance arsenal. Reports later surfaced that several bloggers and activists summoned by the Cybercrime Bureau suspected their devices had been infected by these spyware tools as part of official investigations. The Cybercrime Bureau's chief at the time even defended the use of "ethical hacking" by law enforcement, suggesting a policy of covert digital surveillance against critics.

In 2015, a series of disclosures shone light on the scope of Lebanon's spyware use. In March 2015, Check Point Software exposed "Volatile Cedar," a cyber-espionage campaign originating "likely" from a [Lebanese government agency or allied political group](#). Active since at least 2012, Volatile Cedar deployed custom malware (nicknamed "Explosive") to infiltrate targets including telecom firms, media, military contractors, and others in Lebanon, Israel, Turkey and beyond. Notably, the attackers used an unusual breach-and-pivot method, hacking web servers and moving laterally, instead of simple phishing. This allowed them to steal data and sabotage files on command. Researchers attributed Volatile Cedar to a state-sponsored actor in Lebanon (possibly a unit linked to Hezbollah or Lebanese intelligence) and noted it was the first major spyware campaign traced to Lebanese actors. Around the same time, [Citizen Lab's October 2015 report](#) conclusively attributed FinFisher spyware deployments to specific Lebanese agencies. Their investigation unmasked FinFisher servers on Lebanese networks registered to "General Security" (pointing to GDGS) and to an ISF subdomain. In a published list of FinFisher government users, Citizen Lab named Lebanon's General Security and ISF among the customers of the spyware. This technical evidence, which included IP addresses and domains tied to Lebanese government units, confirmed that both major security branches were running FinFisher for surveillance purposes on their targets. The 2015 leaks and research indicate that Lebanese authorities had procured multiple commercial spyware systems (FinFisher and Hacking Team's RCS) and were conducting espionage operations beyond Lebanon's borders.

2016-2018: Major cyber-espionage campaigns uncovered

Lebanon's digital surveillance capabilities continued to evolve, and by 2017-2018 they became the focus of high-profile revelations. In January 2018, a joint investigation by the [Electronic Frontier Foundation \(EFF\) and Lookout](#) unveiled a sprawling espionage operation dubbed "Dark Caracal." This [campaign](#), which was active since at least 2012, was traced to an office of the General Security Directorate in Beirut.

Researchers discovered that Dark Caracal had compromised thousands of devices in over 21 countries, [stealing “hundreds of gigabytes”](#) of sensitive data. Victims spanned [Lebanon and numerous other nations](#), including the US and others in Europe, the Middle East, and South Asia, and included journalists, activists, lawyers, military personnel, humanitarian workers, and government officials. The stolen information ranged from private messages and call records to documents, photos, audio recordings, and location data.

At the time, Dark Caracal represented a new breed of threat focusing on mobile devices. Its operators created fake versions of popular secure apps (e.g. Signal, WhatsApp, and Tor Browser proxy Orbot) and spread them via social engineering. Unsuspecting targets were lured through WhatsApp messages or Facebook posts to install these trojanized Android apps, which appeared [legitimate](#) but granted the attackers full access once installed. The Dark Caracal Android malware, dubbed “Pallas,” could secretly harvest SMS texts (including from encrypted messaging apps), activate the microphone and camera, and exfiltrate contacts, photos, and even Wi-Fi network data. Complementing it was a suite of desktop malware; the campaign deployed variants of the Bandoor remote access trojan (for Windows) and a multi-platform spyware called CrossRAT (capable of infecting Windows, macOS, and Linux).

The EFF/Lookout investigation provided strong attribution evidence. By correlating Wi-Fi network names and IP addresses, they linked Dark Caracal’s command-and-control servers to a specific Beirut building used by General Security. The implication was that a Lebanese intelligence unit was running the operation, though the researchers allowed for the possibility of a “rogue employee” scenario. When the report broke, Lebanese officials offered tacit admissions alongside denials. General Security chief Major General Abbas Ibrahim insisted the claims were “very exaggerated” and professed “we don’t have these capabilities – I wish we had those abilities”. However, the Interior Minister at the time conceded that the report was “not not true, it’s just overblown”. Local and international civil society reacted swiftly and a coalition of eight rights groups (including Human Rights Watch, SMEX, and others) called on authorities to investigate the “massive espionage campaign” and halt any unlawful surveillance. Despite official equivocation, Dark Caracal was characterized by experts as “one of the most prolific” mobile espionage campaigns ever exposed.

While Dark Caracal was getting global headlines, another Lebanese-linked threat actor remained active under the radar. Volatile Cedar, the campaign first exposed in 2015, did not disappear; it continued covert operations, likely aligned with Hezbollah or state interests. In early 2020, security researchers observed a resurgence of this group, now also called “Lebanese Cedar,” attacking organizations worldwide. A 2021 report by [ClearSky Security](#) revealed that the group had breached at least 250 servers across the US, Europe, and the Middle East by exploiting web server vulnerabilities. The attackers deployed an updated version of their “Explosive” remote access trojan and a custom web shell (“Caterpillar”) to maintain persistence in victim networks. Victims spanned telecom, internet service providers, hosting companies, and critical infrastructure in countries such as the US, UK, Israel, Egypt, Jordan, and Lebanon itself. ClearSky endorsed earlier attribution assessments that this espionage was politically motivated and linked to Lebanon; they noted multiple indications tying the activity to Hezbollah’s cyber unit, given the targeting of Israeli and regional interests and the known Iran-Hezbollah alliance.

2019–2021: Pegasus spyware and transnational targeting

By 2019, the global proliferation of [NSO Group's Pegasus spyware had also touched Lebanon](#). In 2021, investigative reporting revealed that Lebanese figures were among those selected for Pegasus targeting by foreign clients. A leaked list of phone numbers at the heart of the Pegasus Project included [Lebanon's Prime Minister](#) at the time, Saad Hariri, as a potential surveillance target. Hariri's phone number was apparently chosen by the UAE in 2018 and 2019 for monitoring via Pegasus, suggesting a Gulf state's interest in spying on Lebanese political affairs. Additionally, dozens of [Middle East journalists and activists](#) were found to have been targeted with Pegasus. For example, Citizen Lab uncovered a 2020-2021 campaign against *Al Jazeera* staff by Saudi/UAE operators.

Confirmed Pegasus infections in Lebanon began to come to light. In October 2021, Citizen Lab reported that [Ben Hubbard, the Beirut bureau chief of *The New York Times*](#), had been repeatedly targeted and hacked with Pegasus over a three-year span. Hubbard, who frequently reported on Saudi Arabia (and wrote a book on the Saudi crown prince), was first targeted with a spyware-laced SMS in June 2018 and later hit with zero-click iMessage exploits in 2020 and 2021. Forensic analysis confirmed his iPhone was successfully infected in July 2020 and June 2021 with Pegasus, despite Hubbard having earlier complained to NSO about the attempted hacking. Investigators attributed the targeting to the Pegasus operator nicknamed "KINGDOM" linked to Saudi Arabia. Hubbard's case underscored that foreign governments were conducting surveillance operations inside Lebanon's borders (or against those based there) using advanced spyware.

Around the same time, a high-profile human rights defender in Lebanon also fell victim. Lama Fakihi, the head of Human Rights Watch's Beirut office, received an Apple security alert in November 2021, which led to the discovery that her iPhones had been infected with Pegasus at least five times in 2021. Fakihi, a dual US-Lebanese citizen, was [targeted](#) between April and August 2021, while she was investigating the politically sensitive Beirut port explosion of August 2020. A forensic investigation by HRW, peer-reviewed by Amnesty International's Security Lab, found traces of Pegasus's zero-click exploits (including the FORCEDENTRY iMessage vulnerability) on Fakihi's devices. The attacks gave the spyware's operator full access to her phone (camera, microphone, texts, emails, etc.) and by extension to her confidential communications. NSO Group claimed it had "no knowledge" of any active customer targeting a Human Rights Watch staff member and promised to investigate. While the identity of the Pegasus client in these cases was not confirmed in the reports, patterns suggest it may have been a Gulf state actor. The broader context, as HRW noted, is that Pegasus has been repeatedly abused to monitor and silence critics, from journalists to activists, across the region.

The targeting of Fakihi and Hubbard in Lebanon demonstrated that the country had become an arena for foreign digital espionage, with various governments' spyware operations overlapping on its soil. These revelations prompted new calls by civil society to regulate or ban surveillance software. [Human Rights Watch](#) urged a moratorium on spyware sales, emphasizing how such tools were undermining privacy and free expression in Lebanon and beyond.

2022-2025: Ongoing surveillance and recent developments

Even after these exposes, digital surveillance activity involving Lebanon has persisted. In 2022, Microsoft identified a previously [unreported hacking group "Polonium"](#), based in Lebanon and working in coordination with Iranian intelligence. Active since early 2022, Polonium breached or targeted over 20

organizations in Israel (especially in the critical manufacturing, IT, and defense sectors) and at least one regional organization with a Lebanon presence. The attackers leveraged a known vulnerability in Fortinet network appliances to gain initial access, then used cloud services (OneDrive) for command-and-control of their malware. Microsoft assessed with moderate confidence that Polonium was an operational unit in Lebanon being directed by Iran's Ministry of Intelligence (MOIS). Cybersecurity experts noted this case as further evidence of the close collaboration between Hezbollah (or Lebanese proxy actors) and Iran's MOIS in conducting regional cyber operations.

Meanwhile, Lebanon's homegrown spyware campaigns have proven resilient. Despite the public outing of Dark Caracal in 2018, the group was never officially shut down. In mid-2022, an EFF researcher monitoring Dark Caracal discovered a [new live campaign](#) by the group targeting activists and dissidents in Latin America. By seizing control of an unregistered domain left behind by the hackers (a technique called sinkholing), EFF was able to observe Dark Caracal's operations in real time. Over several months, the operators remained oblivious that one of their servers was compromised. During that period, Dark Caracal's malware attempted to infect more than 700 additional devices between March and July 2022, with a focus on countries like the Dominican Republic and Venezuela. This surprising geography suggests Dark Caracal may have evolved into a "cyber mercenary" outfit for hire, conducting spying-for-pay outside its original Middle East focus. EFF's ability to infiltrate the campaign was an unprecedented peek into an active operation and showed that the Lebanese-linked group was still in business, merely shifting tactics and possibly clients.

Over the past decade Lebanon has become both an operator and a target in the digital surveillance ecosystem. Lebanese state security agencies, in particular General Security and ISF, procured and deployed spyware suites like FinFisher and Hacking Team's RCS as early as 2012–2015. They have been implicated in running expansive hacking campaigns (e.g. Dark Caracal) that collected data on thousands of people in Lebanon and around the world. Lebanese political actors such as Hezbollah have likewise been tied to cyber-espionage (Volatile Cedar, Polonium) in service of ideological or foreign agendas. At the same time, foreign governments have conducted digital surveillance in Lebanon, from Gulf states [hacking](#) the phones of Lebanese politicians, journalists and NGO workers with Pegasus, to Israel and Iran engaging in cyber operations that touch Lebanese networks. The technical evidence for these activities comes from leaked company documents, forensic analyses of infected devices, and cybersecurity research linking malware infrastructure to Lebanese entities. Each revelation - FinFisher servers in Beirut, spyware demos in Beirut, Dark Caracal's Beirut nexus, Pegasus infections of Beirut-based targets – adds information that clarify the complexity of Lebanon's surveillance landscape. They confirm a steady evolution of digital surveillance in Lebanon, from modest beginnings ignoring wiretap laws, to purchasing off-the-shelf spyware, to conducting large-scale offensive cyber programs. This chronologically unfolding narrative highlights how confirmed deployments of spyware and espionage tools have eroded the privacy of journalists, activists, dissidents, and even officials in and via Lebanon.

Surveillance of journalists in Lebanon

- **Victims/Targets:** In Lebanon, investigative journalists, activists, and even diplomats have been targeted by advanced spyware in recent years. One prominent example involves a wave of attacks in 2021-2022 using the Candiru spyware (aka "DevilsTongue"). Several Lebanese journalists and political dissidents were secretly infected. For instance, in March 2022, cybersecurity

researchers observed Candiru's spyware being delivered to users in Lebanon via a poisoned Chrome browser update, likely aiming at journalists who reported on Lebanese political corruption. Additionally, in late 2021, a spyware campaign hit devices of activists in Lebanon and the Palestinian refugee community there, using lures on local news sites (a "watering hole" infection strategy). While specific names of Lebanese victims were kept confidential (due to safety concerns), groups like Amnesty International have confirmed that multiple civil society figures in Lebanon were compromised. These targets were individuals critical of governmental or foreign influence in Lebanon, for example, journalists covering human rights abuses or corruption, who would be of interest to state security services.

- **Spying Entity:** The exact actor behind these Lebanese spyware cases remains uncertain, but it is believed to be a state-level entity (or entities). Candiru (an Israel-based company) sells its spyware exclusively to government agencies. Possible culprits include Lebanon's own General Directorate of General Security, which has a history of surveilling journalists (e.g. the "Dark Caracal" espionage exposure in 2018), or foreign intelligence services operating in Lebanon. Microsoft and Citizen Lab, which investigated Candiru, noted at least 100 victims worldwide including in Lebanon and attributed the operations to Candiru clients without naming them. In July 2021, [the US government](#) implicitly fingered such actors when it sanctioned Candiru for enabling "malicious cyber activities" against journalists.
- **Technology Used:** The spyware used is "DevilsTongue," the signature spyware implant of Candiru (a.k.a. Saito Tech). It is comparable to Pegasus in sophistication. DevilsTongue can infiltrate multiple platforms, Windows, iOS, Android, and even cloud accounts. In the Lebanese incidents, the initial attack vector was a zero-day exploit in Google Chrome. Avast (a cybersecurity firm) reported that in early 2022 Candiru was using a then-unknown Chrome vulnerability to silently infect targets in Lebanon, Turkey, Yemen, and Palestine. Once DevilsTongue is installed, it can steal messages, files, passwords and even activate the device's camera and microphone without detection. This spyware bypasses user interaction and uses encryption to communicate with its Command-and-Control servers, making detection hard. The attackers also used "watering-hole" attacks, hacking popular Lebanese news or civil society websites to serve malware to visitors. This indicates a broad net to catch targets who frequent those sites.
- **Confirmation Methods:** The Candiru operations were uncovered by a combination of tech company investigations and cybersecurity research. In July 2021, Microsoft and Citizen Lab released reports on Candiru, after Microsoft discovered and patched exploits that Candiru was using. They documented at least 100 victims of Candiru, including individuals in Lebanon, and provided indicators (like domains and malware hashes). Following that, antivirus company ESET found that certain Middle Eastern news websites (with Lebanese audiences) were compromised to deliver Candiru spyware via injected code. Then, in early 2022, Avast published findings specifically noting attacks on

Lebanese journalists using a Chrome zero-day, which they linked back to Candiru's DevilsTongue. Amnesty International's Security Lab also played a role in Lebanon; in late 2021 Amnesty identified a Pegasus infection attempt on a Lebanese journalist via a malicious WhatsApp message, showing Lebanon was in spyware crosshairs from multiple angles. [The US Department of Commerce's decision](#) to add Candiru to its Entity List in November 2021 further validated these findings, publicly citing Candiru's spyware being used to target journalists and others globally. Therefore, the use of Candiru in Lebanon was confirmed through a mix of forensic analysis (examining malware on affected devices), threat intelligence sharing by companies, and government statements.

- **Actions Taken:** The response to spyware targeting in Lebanon has been mostly international and corporate, with limited domestic action. In July 2021, after Citizen Lab's report, the US government sanctioned Candiru by blacklisting it (as mentioned, putting it on the Entity List). This is an administrative action that makes it illegal for US companies to support Candiru's operations (for example, cutting off its access to software updates or cloud services). Tech companies also responded; Microsoft issued patches and an alert about Candiru, and it joined with Citizen Lab in attributing and calling out the threat publicly. Google, Apple, and Mozilla all rushed to patch the browser and OS vulnerabilities that Candiru was exploiting once those became known. Locally, however, the Lebanese government has not acknowledged any spyware scandal. Some Lebanese NGOs, like Social Media Exchange (SMEX), have demanded the government investigate and protect journalists, but with Lebanon's political turmoil, there's been little traction. Journalists have taken protective action. When Apple began sending spyware warning notifications in late 2021, a handful of Lebanese activists received them; they collectively wrote an open letter asking the government whether it had any role in the espionage. To date, no lawsuit has been filed in Lebanon, partly due to lack of a clear defendant if the perpetrator is a foreign state actor, and partly fear of reprisal. However, Lebanese journalists did collaborate with the [global Pegasus Project](#) in 2021, contributing to exposing how many Lebanese figures (including a major television owner and opposition politicians) appeared on Pegasus target lists.
- **Outcomes/Responses:** Thanks to the spotlight on Candiru, major browsers and operating systems have been hardened, closing the zero-day that was used on Lebanese targets. Candiru's operations were significantly disrupted by the combination of public exposure and the US blacklist. Reports suggest Candiru had to rebrand or downscale after losing access to vital tech partnerships. For Lebanese civil society, an important outcome is that they are now on guard and media houses have started routine device checks and secure communications practices, knowing they are under threat. On the accountability front, there has been no investigation by Lebanese authorities into who deployed the spyware on their citizens.

9.2 Legal Framework

Norms

Lebanon was the first Arab country to adopt a comprehensive interception law - [Law No. 140/1999](#) on the Protection of the Secrecy of Communications. In substance, Law 140 guarantees the secrecy of “internal and external, wired and wireless” communications (telephone, fax, email) and prohibits tapping, monitoring or interception except by law-defined procedures. The law creates two authorization tracks: (i) judicial orders (Articles 2-3) for criminal investigations, which must identify the medium, the offense, the scope and a maximum duration of two months; and (ii) administrative authorizations (Article 9) by the Minister of Interior or Defense with the Prime Minister’s written approval, limited to national security, terrorism, and organized crime, and likewise capped at two months. Decisions are supposed to be verified by an independent high-level judicial commission composed of the heads of Lebanon’s top courts (Article 16).

[The Telecommunications Law No. 431/2002](#) organizes and liberalizes the sector, establishing the Telecommunications Regulatory Authority (TRA) and setting the state’s role over telecommunications services, spectrum, numbering and licensing. While not a surveillance law, it is the backbone of who regulates networks and how operators must comply with state directives. Practically, any systemic access to networks or retention obligations plays out within the Law 431 framework and TRA rule-making space.

Between 2012-2017, practice drifted significantly from Law 140’s individualized, time-bound model. During a 2012 terrorism investigation, security services sought country-wide SMS and internet subscriber datasets (including IPs, usernames, even passwords). The Telecommunications Minister refused, citing privacy, but authorities nonetheless obtained expansive access. In 2013, the Public Prosecutor directed all ISPs and some internet cafés to retain log files for at least one year (usernames, IP addresses, visited sites, protocols, location). From 2014, the Cabinet repeatedly granted blanket, unrestricted access to telecom data (six-month blocks, later four months). Lebanese jurists publicly warned these measures [violated Law 140](#) and far exceeded its two-month, targeted design. These episodes mark a turn toward bulk and ongoing access untethered from individualized suspicion.

The [Access to Information Law No. 28/2017](#) (ATI), its [Implementing Decree No. 6940/2020](#), and a 2021 amendment (Law 233) created a modern right-to-information regime; everyone may request public information, subject to narrow, listed exceptions, and administrations must proactively publish key records. In principle, ATI offers an accountability lever over surveillance governance (e.g., policies, contracts, aggregate statistics), though [implementation](#) has been uneven, as underscored by oversight bodies’ own reporting.

In October 2018, Parliament adopted [Law No. 81/2018 on Electronic Transactions and Personal Data](#). Its data-protection chapter defines core principles (purpose limitation, security, accuracy), creates data-subject rights (access, rectification, objection), and requires filers to declare processing to the Ministry of Economy and Trade (MoET). Certain processing categories demand prior licenses:

- State security processing: joint decision of the Ministers of Defense and Interior
- Criminal-justice data: decision of the Minister of Justice

- Sensitive health/genetic/sexual-life data: decision of the Minister of Public Health.

Other processing generally needs a permit filed with MoET (with specified disclosures), and the law cross-references Law 140 for communications-related surveillance. Penalties include fines and imprisonment for [unlawful processing or disclosure](#). However, no independent data-protection authority was created. Oversight sits within MoET and line ministries, and security-related processing enjoys broad ministerial licensing. These design choices temper the law's ability to constrain state surveillance.

Lebanon adopted a National Cybersecurity Strategy in August 2019, setting policy directions for critical infrastructure, incident response, and capacity building, but [it did not itself change the legal thresholds](#) for interception or spyware use.

Case Law

The Lebanese judiciary's engagement with questions of digital surveillance, device searches, and spyware has been uneven, reflecting broader tensions between formal privacy guarantees and practices of expansive surveillance. The past two decades reveal both moments of judicial progress, where courts invoked Law 140/1999 on the secrecy of communications to protect privacy, and regressions, where courts accepted broad security prerogatives or failed to address state-linked spyware at all. The jurisprudence can be mapped through three key moments: the internationalized proceedings of the Special Tribunal for Lebanon (STL), a landmark domestic ruling on mobile phone searches, and the evolving litigation around fabricated digital evidence in the Ziad Itani affair.

The first major judicial engagement with digital surveillance evidence occurred not in Lebanese courts, but in the Special Tribunal for Lebanon (STL), established by UN Security Council Resolution 1757 to try suspects in the assassination of former Prime Minister Rafik Hariri. In *Prosecutor v. Ayyash et al.*, STL-11-01/T/AC/AR126.9 (28 July 2015), the Appeals Chamber ruled on the admissibility of call data records (CDRs) supplied by Lebanese operators. Defense counsel argued the records had been obtained without [judicial authorization](#) and therefore violated the right to privacy. The Appeals Chamber, however, upheld their use, reasoning that Security Council resolutions provided a sufficient legal basis for the transfer and that the interference with privacy was "provided for by law, necessary, and proportionate" in investigating a mass atrocity. While the STL is not a domestic court, this decision had a profound effect, validating large-scale reliance on telecom metadata from Lebanon and introduced into regional practice a proportionality analysis that would later frame debates on bulk access to CDRs .

Later, a turning point for Lebanese jurisprudence came in [X v. Public Prosecutor, Case No. 313/2015 \(Beirut Misdemeanor Court of Appeals, 14 November 2018\)](#). The case, which also dealt with charges under Article 534 of the Penal Code, raised the question of whether police could search a mobile phone without a warrant. While the defendant was acquitted on other grounds, Judge Rabih Maalouf, in a concurring opinion, explicitly invoked Law 140/1999, which protects the secrecy of communications. He reasoned that a mobile phone constitutes a communications device and therefore cannot be searched absent a judicial order from an investigating judge, supported by a reasoned written decision. Maalouf also stressed that evidence extracted under coercion or torture should be inadmissible. This opinion has been widely cited in legal and civil-society circles as a landmark recognition that digital device searches require the same constitutional protections as communication interception. It signaled a progressive interpretation, [extending privacy rights](#) into the digital age and pushing back against the common prosecutorial practice of accessing phones without warrants.

The [Ziad Itani](#) affair brought into focus how digital surveillance tools can be abused to fabricate evidence. In 2017, the actor and playwright was falsely accused of spying for Israel, based on manipulated electronic communications. Subsequent trials revealed the extent of the fabrication. In *State Security/People v. Elie Ghabash & Suzanne al-Hajj* (Permanent Military Court, 30 May 2019), hacker Elie Ghabash was convicted for fabricating digital evidence, while former ISF officer Suzanne al-Hajj was acquitted of the main charges but convicted for failing to report the information. The court thus recognized the criminal misuse of hacking techniques to produce false digital evidence. Later, in [Itani v. Lebanese State](#), Council of State Decision No. 69/2024–2025 (5 December 2024; published 10 March 2025), the State was held administratively liable for Itani’s torture, violations of his presumption of innocence, and the state’s failure to investigate abuses. The Council awarded compensation (reportedly LBP 480 million), a rare instance of judicial recognition of state accountability in connection with digital-fabrication cases. Together, [these rulings](#) illustrate progress in recognizing harms tied to digital manipulation, even if framed more in terms of torture and abuse of process than as jurisprudence on spyware per se.

Despite high-profile revelations about [Dark Caracal \(2018\)](#), involving Android malware and fake secure messaging apps linked to a General Security building, Lebanese courts have produced no publicly available judgments addressing spyware use, procurement, or remedies. Civil-society groups like SMEX and [Maharat](#) have repeatedly flagged this accountability gap, stressing the absence of judicial or legislative oversight on spyware operations. Similarly, while the verification commission under Law 140/1999 is mandated to oversee administrative interception orders, its deliberations remain opaque. Reports suggest it has occasionally rejected blanket requests (e.g., “all SMS or Skype data”), but no formal case law or published decisions are available. This opacity prevents the development of a transparent jurisprudence on bulk surveillance orders, even as blanket telecom-data requests continued in practice throughout the 2010s.

10. JORDAN

Summary

Legal Framework

Jordan’s legal system grants authorities broad surveillance powers with very limited transparency or oversight. The Constitution (Article 18) guarantees the privacy of correspondence and communications, but allows monitoring “in accordance with the law,” and Jordan’s laws set few firm limits.

The Telecommunications Law of 1995 and its amendments empower the government to issue directives to telecom operators in matters of national security. In practice, the Intelligence Directorate and special police units can require telecom companies to provide call data or tap lines, often based on general State Security Court warrants that are issued in secret. Jordan’s Crime Prevention Law (from 1954) is sometimes used to detain individuals and search their devices without due process under the rubric of preventing crime, effectively bypassing normal procedures.

An important statute is the Defense Law, activated under a state of emergency (as seen periodically, including during COVID-19), which enables the Prime Minister to suspend ordinary laws. This has been interpreted to allow surveillance measures deemed necessary for public security.

Jordan does not have a comprehensive communications interception law made public. Instead, surveillance is governed by internal regulations. Reports indicate that any phone tap in Jordan technically requires approval from the Interior Ministry or a specialized judge of the State Security Court, but in reality, the General Intelligence Department (GID) operates with autonomy and little external oversight.

The Cybercrime Law (enacted in 2015 and expanded in 2023) criminalizes certain online speech and hacking, but does not establish a warrant requirement for government interception of online communications; according to critics, it primarily serves to give authorities tools to penalize dissidents for content. Furthermore, Jordan has no personal data protection law, meaning there is no independent authority to decide how security agencies collect or use citizens' digital data. The absence of data privacy legislation (despite drafts being proposed) leaves a regulatory vacuum.

Jordan has, reportedly, purchased advanced surveillance technology. Leaked records (2014-2019) showed Jordanian agencies obtained spyware and IMSI-catchers. While the government denied illegal use, there is *de facto* legal cover through broad laws like the Protecting State Secrets and Documents Law, which could be interpreted to authorize secret surveillance operations. Oversight of intelligence is entirely within the executive branch and the royal court. Parliament's committees rarely question the GID or PSD (Public Security Directorate) about surveillance practices.

In recent years, as regional instability grew, the government leaned on legal provisions to censor and surveil. In 2020 it ordered internet service providers to block messaging apps during teacher protests (justified under Defence Law orders). The Press and Publications Law and Anti-Terrorism Law also indirectly facilitate surveillance, since they empower authorities to monitor online activity for offenses like insulting the king or "promoting terrorist ideology," effectively legitimizing broad online monitoring.

In summary, Jordan's framework is one where surveillance is largely governed by executive sanction and emergency-style powers. The laws that exist are either silent on oversight or explicitly tilted in favour of state security interests, with the judiciary and legislature having a marginal role. Jordan's commitments under international human rights covenants call for balance, but domestically that balance is skewed towards security, leaving Jordanians with little legal protection if they are placed under digital surveillance or if their communications are intercepted by the state.

Case Law

Jordan's courts have virtually no published jurisprudence addressing or limiting digital surveillance. Unlike some neighbouring countries, there have been no high-profile constitutional cases on privacy or landmark rulings on the admissibility of intercepted evidence. The State Security Court, a military tribunal for national security offenses, often uses evidence from surveillance (wiretaps or hacked messages) in trials of terrorism or sedition cases, and it has never publicly excluded such evidence on privacy grounds. For instance, in a 2015 terrorism trial, transcripts of the defendant's phone calls (obtained by GID without a disclosed warrant) were accepted by the court; the defence's objection on constitutional grounds was simply overruled.

The lack of judicial pushback is partly due to Jordan's legal culture. The courts generally defer to the executive on security matters. In one rare civil case in 2017, a group of activists filed a lawsuit claiming that the government's monitoring of their Facebook accounts and subsequent arrest violated their right

to privacy and free expression. The Amman Court of First Instance, however, dismissed the suit, effectively stating that monitoring public social media for threats was within state authority and did not require judicial pre-authorization. The plaintiffs did not appeal, allegedly fearing retaliation.

When reports emerged that Jordanian activists and even a royal family member had been targeted by Pegasus spyware (as revealed by Citizen Lab in 2021), there was no domestic legal action. No known complaints were filed in Jordan's courts, likely due to fear and scepticism about getting a fair hearing. Internationally, Jordan was called out in a November 2021 joint statement by UN experts condemning the Pegasus targeting of Jordanian dissidents, but internally the judiciary remained silent.

Jordan's judiciary has been seen enforcing laws that punish those who expose surveillance. A notable example took place in 2019, when a journalist who reported on alleged GID phone-tapping practices was prosecuted for "spreading false news" and the court gave him a suspended sentence, signalling that even discussing state surveillance is off-limits.

Overall, the body of case law in Jordan expands state powers or at best leaves them unchallenged. Courts regularly uphold broad interpretations of the Cybercrime Law to convict online critics (implicitly endorsing the continuous monitoring of online speech), while never addressing the legality of the monitoring itself. In the absence of judicial decisions defending privacy, Jordanians have occasionally sought redress through the Royal Human Rights Commission or the Ombudsman's Bureau, but those venues have no binding authority.

10.1 Deployment

Early 2010s: Jordan's adoption of commercial spyware

[Jordan's interest in advanced digital surveillance](#) began to surface in the early 2010s. Leaked correspondence from 2011-2015 revealed that Jordan's General Intelligence Department (GID) was in direct contact with Italian spyware vendor Hacking Team, exploring the use of its Remote Control System (RCS) malware. Internal emails show that Hacking Team's spyware was intended not just for the GID, but also for Jordan's Public Security Directorate (police) and even the military. Around the same period, evidence emerged that Jordan had procured FinFisher (FinSpy), a spyware suite sold by Munich-based Gamma Group. In late 2014, [Citizen Lab's global internet scan](#) identified FinFisher command-and-control servers operating from Jordan, making Jordan one of 32 countries likely using FinFisher for covert surveillance at that time. These findings confirm that by the mid-2010s, Jordanian authorities were equipping themselves with government-grade spyware tools, laying the groundwork for more expansive digital surveillance in the years ahead.

Mid-2010s: Expanding surveillance infrastructure

Throughout the mid-2010s, Jordan continued to build its digital surveillance capabilities. The [2015 breach of Hacking Team](#) further exposed Jordan's role, with the leaked client lists indicating Jordan as a current or former user of Hacking Team's RCS spyware. Although the full extent of Hacking Team's deployment in Jordan remains unclear, Privacy International reported that regular exchanges and a contract were in place, suggesting Jordanian intelligence and law enforcement had operational spyware by this period. Likewise, FinFisher's presence in Jordan persisted. [Citizen Lab](#) noted new FinFisher servers

in Jordan even after Gamma Group's client data was leaked, implying continued use despite the exposure. By the late 2010s, Jordan had also likely acquired cellular interception technology. A 2020 investigative report by *Haaretz* revealed that NSO Group used code names for clients, with Jordan reportedly codenamed "Jaguar" for an [NSO-affiliated Circles system](#) that exploits phone networks to track calls and SMS. Citizen Lab scans did not directly detect a Circles installation in Jordan, possibly indicating such systems were run covertly or via third-country infrastructure.

2019-2021: Pegasus spyware arrives and targets emerge

Jordan's use of NSO Group's Pegasus spyware began to come to light in 2019. [Citizen Lab](#) later determined that a Pegasus operator focusing on Jordan had been active since at least 2018. The first confirmed victim was Hala Ahed Deeb, a prominent Jordanian human-rights lawyer. [Forensic analysis](#) showed her iPhone was infected with Pegasus in March 2021. The hack was uncovered by [Front Line Defenders](#) and Access Now and independently confirmed by Citizen Lab, causing Deeb to describe feeling "violated, naked, and with no dignity" after learning her private data was accessed. Around the same time, evidence pointed to other Pegasus infections in Jordan. Citizen Lab and Amnesty International Security Lab reported that at least four [Jordanian journalists, activists and lawyers](#) had their phones covertly hacked between August 2019 and December 2021. These included anti-corruption activist Ahmed al-Neimat, attorney Malik Abu Orabi, and journalist Suhair Jaradat, among others. Investigators identified two distinct Pegasus operators, which they codenamed "MANSAF" and "BLACKIRIS," believed to be Jordanian government agencies running Pegasus campaigns. The Pegasus infections in this period coincided with rising domestic unrest (e.g. the 2018-2019 protests and Teachers' Syndicate activism) and a broader crackdown on dissent, suggesting that authorities turned to spyware as a new means of monitoring critics. In late 2020, NSO Group's own dealings hinted at Jordan's adoption of Pegasus. Senior [NSO executives](#) travelled to Amman to pitch "new spying technology" to the GID and other officials, reportedly demonstrating Pegasus or related tools for hacking messaging apps. According to sources cited by Axios, those negotiations led to a contract by early 2021.

2021: High-profile surveillance and foreign actors

The year 2021 underscored both the aggressive use of Pegasus within Jordan and the risk of foreign surveillance targeting Jordanians. In July 2021, the Pegasus Project leaks included hundreds of Jordanian numbers, among them people close to King Abdullah II. While being on the leaked list is not proof of infection, it raised alarm that Jordan's leaders and officials were themselves targets of foreign spyware operations. Jordanian lawmakers and media demanded investigations into how "nearly 200 Jordanians' phones" appeared on Pegasus target lists. Separately, in October 2021, a case unfolded in London's High Court where a judge found that Sheikh Mohammed bin Rashid Al Maktoum, the ruler of Dubai, used Pegasus to hack the phones of his [ex-wife Princess Haya of Jordan](#) (the daughter of Jordan's late King Hussein) and her close associates. The court's fact-finding revealed that agents acting for Sheikh Mohammed infected Princess Haya's device and even those of her UK lawyers in 2020, amid a custody dispute, an "unlawful abuse of power" according to the judge. Meanwhile inside Jordan, Pegasus continued to be trained on domestic critics. Front Line Defenders late-2021 investigation (publicized in January 2022) already pointed to a pattern of abuse. They confirmed Pegasus hacks against Deeb and at least one other woman human-rights defender, and warned that "all human rights defenders working against corruption in Jordan" appeared to be under threat.

2022: Investigations confirm government spyware operations

In 2022, digital rights researchers published extensive, peer-reviewed evidence conclusively attributing Pegasus attacks to Jordanian state actors. In April 2022, Citizen Lab and Front-Line Defenders released the “Peace Through Pegasus” report, documenting how at least four Jordanian civil society members were hacked between 2019 and 2021. The report named two Pegasus operator groups likely run by Jordan’s government: MANSAP, active since at least December 2018, and BLACKIRIS, active since around 2020. These operators used SMS messages with spyware links tailored to Jordanian themes, further indicating a domestic hand behind the attacks. [Citizen Lab’s analysts](#) assessed with high confidence that these Pegasus deployments were the work of [Jordan’s security agencies](#). Significantly, this investigation was triggered by a local awareness effect. After Hala Ahed Deeb’s infection was revealed in late 2021, over 60 other Jordanian journalists and activists approached researchers to have their phones examined. Many turned out to be positive for Pegasus traces, reinforcing how widespread the spyware’s use had become. In parallel, credible reports emerged of foreign cyber-espionage attempts inside Jordan. In May 2022, Malwarebytes researchers caught an [Iran-linked hacker group](#) (known as APT34/OilRig) running a phishing attack against a Jordanian government official. The attackers sent a Trojan-infected Excel file (masquerading with the Jordanian Foreign Ministry’s letterhead) to a Foreign Ministry email address, aiming to implant a backdoor on the official’s PC. Malwarebytes attributed the operation to APT34 based on the malware’s code and tactics, noting the group has targeted Middle Eastern governments since at least 2014. While Jordanian authorities did not publicly comment on the incident, its exposure showed that Jordan itself is a target of nation-state hacking, in this case, likely an Iranian espionage operation against Amman’s diplomats.

2022-2023: Widespread targeting of journalists and dissidents

By 2022 and 2023, the picture of digital surveillance in Jordan expanded from isolated cases to a broad pattern of abuse affecting dozens of individuals. In late 2022, Apple Inc. notified certain iPhone users in Jordan that they were targets of “state-sponsored attackers.” [Two Human Rights Watch staffers](#) in Amman, MENA experts Adam Coogler and Hiba Zayadin, received Apple’s threat notifications in August 2023. Upon investigation, HRW’s security team found that Coogler’s personal iPhone (with a Jordanian number) had in fact been infected with Pegasus on October 2-3, 2022. The zero-click exploit used was later linked to NSO’s abuse of Apple’s HomeKit feature, confirming Citizen Lab’s disclosure of that iOS vulnerability around that time. Zayadin’s phone was targeted repeatedly in 2023, though her enabling of Apple’s new Lockdown Mode apparently thwarted those infection attempts. These findings were published by Human Rights Watch in February 2024, alongside the disclosure that at least 33 other Jordanians, including journalists, activists, opposition politicians, and lawyers, were showing evidence of Pegasus targeting between 2019 and September 2023. This “sweeping targeting” was jointly investigated by Access Now and Citizen Lab, amounting to one of the largest documented spyware campaigns in the region.

On February 1, 2024, [Access Now](#) released a comprehensive report titled “Between a Hack and a Hard Place: How Pegasus Spyware Crushes Civic Space in Jordan.” The report identified 35 Pegasus victims in Jordan from 2019–2023, naming 13 of them publicly. Among those confirmed hacked were well-known figures, including journalists from OCCRP (investigative editors Rana Sabbagh and Lara Dihmis were each targeted multiple times), leading human-rights lawyers like Alaa al-Hiyari, women’s rights organizer Manal Kasht, and the HRW staff mentioned above. Many others chose to remain anonymous due to fear

of reprisals. [Citizen Lab](#) independently verified forensic data for 30 of these cases, lending strong credence to the findings. Journalists were the single largest category of [Pegasus targets](#) in Jordan. At least 16 media professionals were attacked, comprising about half of the known victims. For example, veteran journalist Daoud Kuttab (a dual Palestinian-American citizen based in Jordan) was hacked with Pegasus three times between February 2022 and September 2023. Kuttab later recounted how one infection began after he clicked a WhatsApp message from a disguised sender, indicating that some of the Pegasus intrusions in Jordan relied on one-click phishing, in addition to the zero-click exploits used against others.

While the Access Now/Citizen Lab report stopped short of explicitly blaming a particular agency, it noted the Jordanian government is the only actor with an obvious interest and capacity to conduct this widespread domestic surveillance. As HRW observed, it is “difficult to imagine who other than Jordan’s government” would be behind the coordinated hacking of Jordanian civil society. The Jordanian authorities have officially neither confirmed nor denied involvement. However, past incidents strongly imply state responsibility. As the Guardian reported, Jordanian security forces have been “widely suspected” of deploying Pegasus since at least early 2021, when the first cases came to light. In one earlier case, lawyer Hala Ahed (who represented the opposition teachers’ union) was infected in 2021 and then again targeted in 2023, the latter attempt coinciding with renewed government harassment of the Teachers’ Syndicate. Such patterns suggest the hacks aligned with domestic crackdowns.

By the end of the period, international pressure was mounting. [Digital rights NGOs](#) called on Amman to investigate the abuse of spyware against Jordanians and impose a moratorium on its use. “We believe this is just the tip of the iceberg... the true number of victims is likely much higher,” Access Now stated, warning that Pegasus had “staggeringly” enabled repression of Jordan’s civic space.

In sum, confirmed forensic evidence shows that from 2019 through 2023, digital surveillance in Jordan transitioned into a pervasive, invasive campaign, primarily carried out by Jordan’s own security apparatus using foreign-made spyware. Journalists, human-rights defenders, union organizers, and international NGO staff were systematically spied upon with Pegasus, a trend that mirrors other authoritarian uses of the tool around the world. At the same time, Jordanians also fell victim to external surveillance operations.

10.2 Legal Framework

Norms

Jordan’s approach to digital surveillance and spyware regulation reflects a blend of national security priorities, cautious modernization, and evolving legal frameworks. While the country has not enacted a single, comprehensive surveillance law, several statutes and policy instruments collectively shape the legal landscape.

The cornerstone of Jordan’s cybersecurity governance is the [National Cybersecurity Strategy 2025–2028, approved by the National Cyber Security Centre \(NCSC\)](#). This strategy outlines four strategic objectives: strengthening institutional capabilities, securing digital services, attracting global cybersecurity investment, and positioning Jordan as a regional innovation hub. Though not a law, it sets the tone for [future regulatory efforts](#) and emphasizes performance tracking and accountability across public and private sectors.

In parallel, Jordan has taken steps to regulate digital assets and data environments that intersect with surveillance concerns. The Law Regulating Dealings in Virtual Assets No. 14 of 2025 establishes a legal framework for cryptocurrencies, NFTs, and other digital instruments, excluding central bank digital currencies and securities regulated by the Central Bank of Jordan and the Jordan Securities Commission (JSC). While not directly targeting spyware, the law reflects the government's intent to formalize digital governance and mitigate financial crime risks.

Oversight of surveillance activities remains largely within the purview of security agencies, including the General Intelligence Department and the Ministry of Interior. These bodies operate under broad mandates, and while judicial oversight exists in theory, the legal thresholds for interception and spyware deployment are not clearly codified. Jordan has yet to establish an independent data protection authority or pass a dedicated privacy law or data-protection law.

Transparency and accountability mechanisms are limited. The country does not currently require public disclosure of spyware procurement or usage, and there is no legal obligation to notify individuals targeted by surveillance. Civil society groups have raised concerns about the potential for abuse, especially in the absence of judicial review or independent oversight.

Overall, Jordan's legal standards for digital surveillance and spyware remain fragmented. The 2025 cybersecurity strategy and virtual asset law signal a shift toward structured digital governance, but gaps persist in privacy protections, transparency, and institutional checks. As regional and global norms evolve, Jordan faces growing pressure to align its surveillance practices with international human rights standards.

Case Law

In recent years, Jordan has become a focus of international concern regarding digital surveillance and spyware, particularly due to revelations of Pegasus spyware infections among civil society actors. Yet, when one turns to the courts for jurisprudential guidance, the reality is the absence of explicit judicial rulings that address spyware or surveillance legality. Instead, Jordan's courts have developed their engagement with digital rights largely through cybercrime prosecutions and state security cases, leaving fundamental questions about surveillance and privacy unanswered.

Between 2019 and 2023, independent investigations by Citizen Lab, [Access Now](#), Amnesty International, and others confirmed that at least 35 journalists, lawyers, and human rights defenders in Jordan had been targeted by NSO Group's Pegasus spyware. The earliest confirmed infection dates to March 2021, when human rights lawyer Hala Ahed was attacked.

Despite this mounting body of evidence linking spyware deployment to Jordanian authorities, no court in Jordan has heard a case on the legality of spyware use, nor has any judicial decision provided remedies to victims. Civil-society organizations, such as [HuMENA for Human Rights and Civic Engagement](#), describe this as a profound accountability vacuum, a silence that allows spyware practices to proceed without legal scrutiny.

Where Jordanian courts have been active is in cases under cybercrime legislation. The most significant recent development is the adoption of [Cybercrime Law No. 17 of 2023](#), which came into force in September 2023.

This law criminalizes broadly defined acts such as publishing “fake news,” promoting “immorality,” insulting religion, and using VPNs without authorization. It also empowers prosecutors to initiate cases even without a formal complaint, particularly where government entities are involved. By mid-2024, the [law](#) was already being used to arrest journalists, human rights activists, and protesters for online expression, often accompanied by warrantless seizures of devices and coerced interrogation.

While not directly about spyware, these cases highlight how the judiciary interacts with the digital sphere, prosecuting expression rather than scrutinizing surveillance. The result is a body of case law that reinforces restrictions on speech and association, while leaving the legality of state digital surveillance practices untouched.

Chapter 3. Curbing the threat - international responses

3.1 United Nations

Over the past three decades, the United Nations (UN) has built an increasingly detailed guardrail system against abusive digital surveillance, evolving from broad privacy principles to technology-specific safeguards and oversight mechanisms. These efforts began with the 1990 'fair-information guidelines', then accelerated after 2013 with the General Assembly's (UNGA) "privacy in the digital age" track (series of subsequent resolutions), which translated ICCPR protections into concrete tests of legality, necessity, proportionality, transparency, and effective remedy.

Institutionally, the Human Rights Council (HRC) created dedicated mandates and affirmed technical protections like encryption and anonymity as rights-enabling, while successive analyses expanded the lens from state practices to private surveillance vendors and, more recently, AI-enabled monitoring and spyware.

By 2024-2025, proposals to update the UN's baseline data-protection guidance, the adoption of a global cybercrime instrument, and Security Council attention to spyware signal a system that now links human rights, rule of law, and international security. Read together, these milestones show steady, incremental tightening of standards and accountability expectations across the UN system.

Each milestone tightened the test of legality, necessity, proportionality, oversight, and remedy, expanded it to new technologies and actors, and pressed states to translate norms into enforceable domestic laws and independent controls.

Milestones

As early as 1990, the UN General Assembly's [*Guidelines for the Regulation of Computerized Personal Data Files*](#) (45/95) set early global privacy baselines - lawfulness, purpose limitation, data quality, security, access, and independent supervision. Although pre-Internet, they established the architecture (principles and oversight) later used to assess state surveillance against human rights law.

The Guidelines set out fair-information principles that national laws should guarantee for any computerized personal data file: data must be collected and used lawfully and fairly; kept accurate, relevant, up to date, and limited to a specified, legitimate purpose that is made known to the data subject; individuals have the right to know whether they are in a file, to obtain their data in intelligible form without undue delay or cost, and to seek rectification or erasure of unlawful, unnecessary, or inaccurate entries; sensitive data that may enable discrimination (e.g., racial or ethnic origin, political opinions, religious or other beliefs, sex life, trade-union membership) should not be compiled except under tightly limited circumstances; any departures from these principles must be expressly set out in law, strictly necessary for aims such as national security or the rights of others, and accompanied by appropriate safeguards; files must be protected by appropriate security against unauthorized access, misuse, loss, or destruction; each country should designate an impartial, independent supervisory authority empowered to oversee compliance and ensure sanctions and remedies; cross-border data flows should be free where comparable protections exist, with limitations imposed only to the extent privacy protection demands.

More than 20 years later, in the wake of Snowden resolutions, [UNGA resolution 68/167](#) affirmed the same rights people enjoy offline must be protected online, including the right to privacy; the resolution voices deep concern about the negative human-rights impact of surveillance, interception of communications and collection of personal data, including when conducted extraterritorially; it calls on all States to respect and protect privacy, end violations, and align national laws with international human-rights obligations. The resolution urges States to review their surveillance-related procedures, practices, and legislation, including mass surveillance and mass data collection, with a view to ensuring full and effective compliance, and to establish or maintain independent and effective oversight mechanisms capable of ensuring transparency and accountability, alongside access to remedies. The resolution also requests the UN High Commissioner for Human Rights (OHCHR) to report on the issue and invites continued consideration within the UN system.

In response to this request, the OHCHR's 2014 report [The right to privacy in the digital age \(A/HRC/27/37\)](#) anchors assessments in ICCPR article 17's tests of legality, necessity and proportionality, insisting that limitations be set out in accessible, precise law, serve a legitimate aim, and use the least intrusive means; otherwise, interferences are arbitrary or unlawful. It rejects a content/metadata split, explaining that aggregated communications data can reveal intimate patterns and that any capture or retention of such data is an interference with privacy, with the very existence of mass-surveillance regimes triggering that interference. The report clarifies extraterritorial duties: when a State exercises power or effective control over communications infrastructure or over companies that control data, its human-rights obligations apply beyond its borders. It calls for robust procedural safeguards and independent, properly resourced oversight - drawing on judicial, parliamentary and specialized bodies - and for effective remedies that hinge on notice, standing, and enforceable redress. Recognizing governments' reliance on the private sector, it applies the UN Guiding Principles on Business and Human Rights to vendors and intermediaries, urging due diligence, transparency, and avoidance of complicity in unlawful surveillance. The conclusion presses States to review and reform laws, increase transparency, and strengthen oversight and remedies to make these standards real in practice.

[UNGA Resolution 69/166](#) reinforced this agenda. It largely reaffirms 68/167 but adds several concrete guardrails that go beyond both 68/167 and the OHCHR baseline set in A/HRC/27/37. In the operative text it specifies that surveillance oversight must be not only independent and effective but also "adequately resourced and impartial," and it adds a fresh instruction for States to ensure access to an effective remedy for individuals subjected to unlawful or arbitrary surveillance - two clarifications that operationalize the legality/necessity/proportionality tests elaborated by OHCHR in 2014. In the preamble, 69/166 tightens the requirement that any surveillance rest on a publicly accessible, clear, precise, comprehensive and non-discriminatory legal framework, explicitly recognizes that aggregated metadata can reveal personal information, and brings in the responsibility of business enterprises to respect human rights, as well as attention to risks faced by human rights defenders and the need for [counter-terrorism measures](#) to comply with international law - elements not spelled out in 68/167. Finally, it encourages the Human Rights Council to remain seized of the issue and to consider establishing a special procedure on the right to privacy, which the HRC soon did by creating the Special Rapporteur on [privacy mandate](#) - thereby adding an institutional follow-up mechanism that 68/167 lacked (see below).

With this, the UN's "privacy in the digital age" track was launched and is an ongoing line of work, through which the General Assembly (and, in parallel, the Human Rights Council and OHCHR) develops

and updates global human-rights standards for privacy, surveillance and data use in modern technologies; the “track” refers to the UN’s recurring cycle of resolutions and expert reports that applies ICCPR privacy guarantees to contemporary tech and surveillance practices, and keeps refining the guardrails as technologies evolve.

In 2015, [HRC resolution 28/16](#) created the Special Rapporteur on the right to privacy, ensuring sustained, expert monitoring. In parallel, the Special Rapporteur on freedom of expression’s report on encryption and anonymity (A/HRC/29/32) recognized secure communications as essential to privacy and expression, urging that any limits meet strict necessity and proportionality, thereby turning technical protections (encryption) into human-rights safeguards.

The following year, [Resolution 71/199](#), beyond reaffirming previous documents, expressly links privacy to freedom of expression, peaceful assembly and association, framing privacy as “one of the foundations of a democratic society.” It flags the growing sale and multiple resale of personal data without free, explicit and informed consent. The Resolution deepens on the State-business interface, calling on States not to require companies to take steps that arbitrarily or unlawfully interfere with privacy; to legislate against unlawful/arbitrary personal-data handling by governments, companies and private organisations; and to consider measures enabling corporate transparency reports. It also directly tasks business enterprises to meet their responsibility to respect human rights (per the UNGPs), inform users about data practices, and work toward secure communications. Additional novelties include emphasis on particular impacts on women, children and vulnerable groups.

OHCHR’s [2018 report](#) (A/HRC/39/29) provides detailed guidance on prior authorization, independent and adequately empowered oversight, transparency (including user notification and public reporting), and effective remedies. It addresses the modern data ecosystem, treating bulk collection, metadata analysis and data-intensive technologies, as privacy interferences. The report reinforces the importance of applying the UNGPs to platforms, vendors and intermediaries (including as regards to due diligence, resisting overbroad demands, and clearer disclosures). The report addresses intelligence sharing, urging that cooperation rest on a clear statutory basis with strict limits and independent supervision. It also engages emerging cross-border access to data, cautioning that expanding investigative powers and transnational requests must be bounded by the same human-rights tests.

UNGA [resolution 73/179](#) reaffirmed the digital-age privacy track, noting concern about “profiling, automated decision-making and machine-learning technologies” and their impact on the right to privacy, and by encouraging continued UN consideration of these issues.

The Special Rapporteur on Freedom of Opinion and Expression’s [report A/HRC/41/35](#), presented to the HRC in 2019, shifts the focus from state surveillance in the abstract to the private surveillance industry and its supply chains, and sets out a concrete regulatory blueprint. It documents how commercially sold spyware and related tools enable targeted attacks on journalists, activists, and others, and then proposes specific state and corporate duties: an immediate moratorium on the global sale and transfer of these tools until rigorous human-rights safeguards are in place; tighter export-licensing controls; requirements for independent, prior authorization and strict oversight of any use; and enforceable human-rights due diligence by vendors, including “human rights by design,” transparency reporting, contractual clauses restricting customization/servicing that would facilitate abuses, and effective grievance pathways. It also surfaces neglected risk amplifiers - like the unregulated market in software vulnerabilities - and calls for governance of that [ecosystem](#), linking security practice to rights protection.

[UNGA 75/176](#) explicitly condemns government hacking and the unlawful use of biometric technologies, alongside unlawful or arbitrary surveillance and interception, as “highly intrusive” acts that violate privacy that can also interfere with freedom of expression, assembly/association, and religion, including when done extraterritorially or on a mass scale. It strengthens the provisions on state-business interface by urging States to adopt legislation, policies, and remedies to ensure that business enterprises (including platforms) respect privacy throughout the design, development, deployment, and evaluation of technologies, “including AI”. The resolution moreover builds on language on gender, including stressing “the need to address prevailing challenges to bridge...the gender digital divide[s].” While reaffirming protection for technical safeguards (encryption, pseudonymization, anonymity), the [resolution](#) reiterates that States should not interfere with such solutions, helping carry forward and consolidate the pro-encryption line set by previous iterations of the text.

[OHCHR’s 2021 report](#) *The right to privacy in the digital age* (A/HRC/48/31) moves the UN privacy track decisively into the AI era. It centres AI’s impacts on privacy and related rights and urges States to ban AI applications that cannot be operated in compliance with international human-rights law and to impose moratoria on high-risk systems until robust safeguards exist. The report identifies remote biometric recognition in public spaces as a uniquely intrusive form of surveillance and calls for a specific moratorium on its use pending demonstrable compliance with privacy/data-protection standards and the absence of accuracy and discrimination problems. It operationalises responsibilities across the entire AI lifecycle, recommending comprehensive human-rights due diligence by both States and businesses when acquiring, developing, deploying, and operating AI, including prior assessment, ongoing monitoring, transparency, and accountability measures.

The subsequent [OHCHR’s report A/HRC/51/17](#), from 2022, pivots the UN privacy track from general AI-era risks (A/HRC/48/31) to three concrete fronts: the abuse of intrusive hacking/spyware tools, the centrality of strong encryption, and the risks of widespread public-space monitoring that can enable systems of pervasive surveillance and control. In doing so, it tightens the guardrails around the most acute, real-world practices then emerging from the Pegasus revelations and similar cases. The report argues that government hacking is uniquely invasive because it can compromise entire devices, exposing communications, contacts, location, and sensors; even the existence of such programmes can chill expression and civic life. It stresses that encryption is essential to the enjoyment of privacy and related rights and should not be weakened or undermined by law or design. And it warns that mass or persistent monitoring of public spaces, especially when combined with advanced analytics, can create architectures of control incompatible with international human-rights law unless subjected to strict legality, necessity, proportionality, transparency, and independent oversight. OHCHR calls for an immediate moratorium on the sale, transfer, and use of hacking/spyware tools until robust human-rights safeguards are in place, alongside hard limits in domestic law: prior authorization by an independent and impartial authority; strict targeting; tight time limits; secure logging; post-fact notification and effective remedies; and meaningful, well-resourced external oversight. It urges states to protect and promote end-to-end encryption, avoid measures that would weaken it, and ensure companies are not compelled to build systemic backdoors. For public-space surveillance, it recommends necessity- and proportionality-based restrictions, rigorous impact assessments, and transparency sufficient to allow public scrutiny. The report also presses for export-control discipline and corporate human-rights due diligence across the spyware supply chain, and for governance of vulnerability handling to avoid state stockpiling that endangers security for all.

In 2024, the Right to Privacy Special Rapporteur proposed updating the [1990 Guidelines](#) (A/79/173) so baseline principles reflect today's data ecosystems and surveillance capabilities, connecting legacy fair-information rules to modern realities.

In the same year, [the UN Cybercrime Convention](#) was adopted by UNGA (Dec 24, 2024), a cooperation instrument whose eventual safeguards and implementation will materially affect surveillance and e-evidence practice. Many stakeholders have urged robust human-rights clauses in its application (see Box 1 below).

On 14 January 2025, the United States convened an [Arria-formula meeting of the UN Security Council](#), co-sponsored by Australia, Austria, Canada, Estonia, Finland, France, Japan, Latvia, Lithuania, the Netherlands, Norway, Poland, the Republic of Korea, Sweden and the United Kingdom, to examine how the proliferation and misuse of commercial spyware threatens international peace and security, with states and expert briefers detailing harms to journalists, human-rights defenders, diplomats, UN personnel and elections, as well as cross-border destabilization risks and diplomatic incidents. Delegations' statements (including from Australia, Slovenia, Italy, Ukraine, Guyana and Russia) emphasized accountability for unlawful hacking and device compromise, stronger export-control and procurement due-diligence regimes, transparency around government spyware use, support for victims, and the need to balance cybersecurity with human rights, while a U.S. readout framed next steps around policies to discourage misuse. Although Arria meetings are informal and non-binding, bringing spyware onto the Council's peace-and-security [agenda](#) marked a notable shift from the human-rights track to a security frame, reinforcing momentum for tighter safeguards against digital surveillance across national laws and international cooperation.

Box 1

The UN Cybercrime Convention

The treaty's scope is broad. Beyond creating cyber-offences, it explicitly covers the "collecting, obtaining, preserving and sharing of evidence in electronic form" for criminal cases, and it adds a general human-rights clause requiring implementation consistent with international human-rights law (including expression, assembly and association rights). Those two anchors - Article 3 on scope and Article 6 on rights - frame how the more intrusive procedural powers should operate.

Domestically, Chapter IV requires States to establish a full toolkit for handling electronic evidence. That includes expedited preservation of stored data (Art. 25) and partial disclosure of traffic data to trace a communication path (Art. 26); production orders for stored data and subscriber information (Art. 27); search and seizure (or similar access) to systems and storage media, plus authority to compel "any person who has knowledge" of a system or its protective measures to provide information needed to carry out those searches (Art. 28(4)); real-time collection of traffic data (Art. 29); and real-time interception/recording of content for a range of serious crimes (Art. 30). Service providers can be required to keep such orders confidential (Arts. 29(3) and 30(3)). Notably, Article 23 applies these powers not only to convention offences but also to "other criminal offences committed by means of" ICT

systems and to collecting e-evidence for any criminal offence, significantly widening when surveillance-type powers may be used.

Internationally, Chapter V builds a cooperation layer that also affects surveillance. Article 41 sets up a 24/7 point-of-contact network that, among other things, can facilitate technical advice, preservation requests, evidence collection, locating suspects, and even “the provision of electronic data to avert an emergency,” with “emergency” defined as a significant, imminent risk to life or safety (Arts. 41(3)(e), 2(o)). Articles 42–46 create expedited mutual legal assistance (MLA) for preserved data, access to stored data, and even real-time traffic-data collection and content interception; preservation assistance cannot be refused for lack of dual criminality (Art. 42(4)). Article 40 lays out the general MLA framework (central authorities, confidentiality, refusal grounds, etc.). Together, these provisions streamline cross-border requests for data and live interception support.

Safeguards do appear, but they sit largely at a principles level and depend on national law. Article 24 requires that procedural powers be subject to domestic “conditions and safeguards” that protect human rights and incorporate proportionality, including judicial or other independent review, effective remedies, and limits on scope and duration. Article 36 adds data-protection guardrails for personal data exchanged through cooperation (e.g., only transfer consistent with domestic and applicable international law; ensure “effective and appropriate safeguards”; and restrict onward transfers without the original State’s authorization). MLA may be refused where requests would prejudice sovereignty or essential interests, or where there are substantial grounds to believe a request is discriminatory (Art. 40(21) and (22)). States may also reserve how widely they apply certain real-time powers (Arts. 23(3), 29–30). The net effect: robust new channels and tools for surveillance-adjacent activities, bounded by baseline proportionality and privacy commitments whose strength will hinge on each country’s implementing law and practice.

Several civil-society analyses have flagged that provisions like Article 28(4) (compelling knowledgeable persons to assist searches) and the “any criminal offence” e-evidence hook could enable expansive surveillance unless tightly constrained in domestic law - points to watch as States [implement](#) the treaty.

3.2 European Standards

Norms

The [1950 European Convention on Human Rights \(ECHR\)](#) establishes in its Article 8 the right to privacy and the conditions under which the State may interfere on it - “in accordance with the law” and “necessary in a democratic society” - the bedrock standard later applied to surveillance regimes.

In 1981, the Council of Europe adopted [Convention 108](#), the world’s first binding data-protection treaty; it requires domestic laws with core principles (lawfulness, purpose limitation, data minimization, oversight, remedies) across public and private sectors. These principles are foundational for surveillance limits on personal-data processing.

This document was followed by the [1987 Recommendation R\(87\)15](#) on Police Data by the Council of Europe. It provided early sectoral guidance subjecting police processing to strict data-protection principles (purpose limitation, accuracy, retention limits), influential across Europe.

Almost ten years later, the [Data Protection Directive 95/46/EC](#) was adopted by the EU in 1995. The Directive is an EU-wide baseline for personal-data processing and transfers; later replaced by the GDPR (see below) but pivotal for surveillance-relevant safeguards in administrative and commercial contexts.

The Data Protection Directive was followed by two others also relevant to digital surveillance - ePrivacy Directive [2002/58/EC](#) and the Data Retention Directive [2006/24/EC](#), respectively adopted in 2002 and 2006. ePrivacy is a *lex specialis* for electronic communications, referring to confidentiality of communications and traffic/location data. According to it, Member States' security measures must respect necessity and proportionality - central to later court rulings on data retention. The Data Retention Directive mandated retention of traffic/location data for public-security purposes; ultimately annulled in 2014 for disproportionate interference with fundamental rights.

[EU's General Data Protection Regulation](#) (GDPR) was passed in 2016 (Regulation (EU) 2016/679) along with the [Law Enforcement Directive](#) (LED) (Directive (EU) 2016/680). GDPR modernizes EU data-protection rules (legal bases, DPIAs, accountability, independent oversight) that also covers surveillance uses of personal data in non-law-enforcement contexts; the Law Enforcement Directive sets specific rules for police/judicial processing. Together they provide core horizontal safeguards across Europe. The LED is part of the EU's data protection reform, beside the GDPR. While the GDPR applies to the processing of personal data in general, the LED focuses specifically on the processing of personal data by law enforcement authorities for law enforcement purposes. The [LED also incorporates some provisions and concepts from the GDPR](#), but it also has its own unique rules tailored to the specific needs of law enforcement.

Under the GDPR, digital surveillance by public and private actors is constrained by a set of interconnected duties and rights: it applies to processing in or targeting the EU - including non-EU entities that "monitor the behaviour" of people in the Union - while excluding national-security activities and assigning criminal-law enforcement to a separate regime (the Law Enforcement Directive); once in scope, surveillance must satisfy the core principles of Article 5 (lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity/confidentiality) and rest on a valid legal basis under Article 6, while processing of special-category data such as biometrics is generally prohibited unless a narrow exception in Article 9 applies, which is pivotal for facial-recognition or other biometric monitoring. Individuals gain powerful checks on [surveillance](#) through transparency and access rights (Arts. 12–15), rectification, erasure and restriction (Arts. 16–18), data portability (Art. 20) and the right to object (Art. 21), plus a specific protection against decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects (Art. 22). Controllers must embed safeguards "by design and by default" (Art. 25) and run data-protection impact assessments where surveillance is high-risk - explicitly including "systematic monitoring of a publicly accessible area on a large scale" - and consult the regulator if residual risk remains (Arts. 35(3)(c) and 36); they must also ensure security (Art. 32) and notify breaches to regulators within 72 hours and, where relevant, to affected people (Arts. 33–34). Cross-border data transfers that could expose EU data to third-country government access are only permitted under Chapter V (Arts. 44–49), which - after the Court of Justice's Schrems II ruling invalidated Privacy Shield - require case-by-case assessments and,

where needed, “supplementary measures” per EDPB [guidance](#). Oversight and enforcement structures are robust: independent supervisory authorities wield investigative and corrective powers (Art. 58), cooperation and consistency mechanisms align decisions across the EU (Chapter VII), and serious infringements can attract fines up to 4% of global annual turnover (Art. 83). Member States may legislate targeted restrictions of certain GDPR rights (Art. 23), but only if they respect the essence of fundamental rights and meet strict necessity and proportionality tests - guardrails that are central whenever surveillance is justified on public-interest grounds

The [2016 PNR Directive \(EU\) 2016/681](#) permits use and retention of airline passenger name records for serious crime/terrorism with safeguards; later tempered by proportionality case-law (see below). The PNR Directive is one of the few EU-wide laws that authorizes large-scale, security-driven data collection. It requires airlines to send Passenger Name Record data to national Passenger Information Units, but confines processing strictly to terrorism and “serious crime,” builds in a Data Protection Officer and independent supervisory oversight, mandates logging/auditability, and bars the use of sensitive data (race, politics, religion, health, sexual life/orientation) with immediate deletion if received. The Directive sets a retention ceiling of five years with de-personalisation after six months, and requires human review of any automated matches before authorities act - plus stricter gate-keeping for any disclosure of full, unmasked data after the first six months. Together these provisions create a test-bed for what proportionate, reviewable, and time-bounded surveillance looks like in practice.

In 2018, [updates](#) to the Council of Europe’s data-protection convention (Convention 108) were introduced. The [2018 protocol](#) modernising Convention 108 reinforces safeguards that are directly relevant to digital surveillance. It updates core principles (lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limits) and requires a clear legal basis for processing, with expanded transparency duties toward individuals. It adds stronger protection for sensitive data by explicitly covering biometric, genetic and criminal-justice data, permitting their processing only where law provides “appropriate safeguards” to prevent risks like discrimination. On oversight and user control, it introduces data-breach notification to supervisory authorities where rights may be seriously affected; guarantees rights to explanation/insight into the reasoning behind automated processing that affects a person; and recognises a right not to be subject to a decision based solely on automated processing without their views being considered - important guardrails for AI-enabled monitoring. It embeds accountability, privacy by design and by default, and risk/impact assessment obligations (DPIA-type, see Box 2 below) before high-risk processing begins, and it extends duties to processors as well as controllers. Supervisory authorities gain clearer independence, sanctioning and cooperation powers, while a strengthened Convention Committee can evaluate Parties’ implementation - a follow-up mechanism that helps turn paper rights into practice. For national-security/defence processing, the modernised text makes plain that any restrictions must still be subject to independent and effective review and supervision. Finally, it modernises cross-border data flows: transfers between Parties should generally be free (all Parties share a common baseline), while transfers to non-Parties require an “appropriate level” ensured by law or binding safeguards (e.g., standard clauses), with an anti-circumvention exception to stop routing data abroad to evade protections.

In 2020, the European Data Protection Board (EDPB) passed [Guidelines 3/2019](#) on Video Devices. Guidelines 3/2019 explain how the GDPR applies to video surveillance, insisting that any recording be strictly necessary and proportionate to a defined purpose, rest on a valid legal basis (often legitimate interests or a public task), and be transparent to people through clear signage and notices. They stress

data-minimisation (e.g., restricting fields of view, masking/pixelation, short retention, avoiding audio unless truly needed), and note that using video to uniquely identify individuals may trigger “special category” (biometric) rules that require additional safeguards. Controllers must run DPIAs (see Box 2 below) for high-risk uses such as large-scale, systematic monitoring of publicly accessible areas, enable data-subject rights (access, objection, erasure), and address issues like joint controllership and processor duties; household exemptions are narrow, and “fake” cameras fall outside GDPR because no personal data are processed. Overall, the Guidelines turn abstract GDPR principles into concrete guardrails for CCTV, dashcams, body-worn cameras, drones and “smart” video systems - limiting surveillance to what is lawful, necessary, and rights-respecting.

[Guidelines](#) were also adopted in 2021 by the e Consultative Committee of Convention 108 on Facial Recognition (T-PD(2020)03rev4, adopted 28 Jan 2021). The Guidelines treat facial recognition (FRT) as a high-risk surveillance technology and lay out human-rights guardrails for both public and private use. They require a clear, use-specific legal framework and insist deployments be strictly necessary and proportionate - with some uses to be strictly limited or even prohibited by law - given the serious risks when FRT is integrated into surveillance systems. The Guidelines curb function creep by restricting reuse of existing image databases, and they confine private-sector use largely to controlled environments on the basis of explicit, specific, freely given consent with genuine alternatives. For law enforcement, covert live FRT is at most permissible to avert an imminent and substantial public-safety risk and must be documented. Across all contexts they mandate transparency, public involvement, DPIAs and periodic re-assessment, data-protection by design/default, and accountability (including accuracy and bias-mitigation duties), while reinforcing data-subject rights and safeguards around automated decisions.

Box 2

Data Protection Impact Assessment (DPIA)

A DPIA is a mandatory, pre-deployment risk assessment under the GDPR whenever a processing operation is likely to result in a high risk to people’s rights - especially with new technologies, large-scale or systematic monitoring of public spaces, or uses of special-category data like biometrics. It must describe the processing, assess necessity and proportionality, identify risks to rights and freedoms, and set out measures to mitigate them; if high risk remains, the controller must consult the data-protection authority before going ahead.

In practice, video surveillance and facial recognition almost always trigger a DPIA: GDPR Article 35 names large-scale public-area monitoring; the EDPB’s Video Devices Guidelines reinforce DPIA expectations for CCTV/drones/bodycams; and Convention 108’s Facial Recognition Guidelines make prior DPIAs (with transparency and periodic re-assessment) a baseline safeguard. For police/criminal-justice uses, the Law Enforcement Directive (EU) 2016/680 has a parallel DPIA requirement ([Art. 27](#)). And looking forward, the EU AI Act adds a complementary fundamental-rights impact assessment for deployers of certain high-risk AI systems in the public sector - sitting alongside, not replacing, GDPR/LED.

[Regulation \(EU\) 2021/821](#) - the recast Dual-Use Regulation - is the EU's core export-control law for goods, software and technology with both civilian and military uses, covering physical shipments and intangible transfers (e.g., remotely supplying code or know-how). Its legally binding Annex I is the control list that tells exporters which items need a licence when leaving the EU; the Commission updates Annex I by delegated acts to mirror changes agreed in multilateral regimes (Wassenaar, Australia Group, MTCR, NSG), and a subset in Annex IV is so sensitive that some intra-EU movements are also controlled. For digital surveillance, the recast adds Article 5's "catch-all" provision: even if a cyber-surveillance item (e.g., spyware, interception systems, forensic tools) is not listed in Annex I, authorities can still require a licence where there is a risk of internal repression or serious human-rights or IHL violations. Exporters must run human-rights due diligence and notify authorities if red flags arise; Member States can impose national controls for public-security or human-rights reasons, and [EU guidance \(most recently expanded in 2024\)](#) explains how to assess and mitigate those risks. The recast also strengthens oversight of brokering and technical assistance, expands transparency and enforcement coordination, and encourages pushing human-rights controls into the multilateral lists. Annex I's baseline controls plus Article 5's risk-based catch-all make 2021/821 the EU's principal instrument for constraining the [export and facilitation](#) of digital-surveillance capabilities in a way that embeds privacy and human-rights safeguards.

In 2023, the EU "e-Evidence" package was adopted. It creates European Production/Preservation Orders for cross-border access to electronic evidence from service providers, with judicial authorization, notice/grounds, remedies and conflict-of-law rules. It builds a procedural channel for criminal cases that lets a judge or prosecutor in one Member State order a service provider anywhere in the EU to produce or preserve stored electronic data - while hard-wiring privacy guardrails. The [Regulation \(EU\) 2023/1543](#) creates European Production Orders (EPOC) and Preservation Orders (EPOC-PR) for three data categories - subscriber, traffic, and content data - and requires a case-by-case necessity and proportionality assessment; judge review is mandatory for traffic (beyond basic identification) and content data, reflecting their higher intrusiveness. It also clarifies important limits: it authorises no interception, imposes no general data-retention, and does not require decryption; orders target data stored at receipt and may carry tight deadlines (generally up to 10 days, or 8 hours in emergencies). The Regulation adds a notification mechanism to an "enforcing" authority for more sensitive orders so that privileges, press freedom and immunities can be checked, and it even allows defence requests for exculpatory evidence - features that temper intrusive powers. The companion [Directive \(EU\) 2023/1544](#) makes the system workable by forcing in-scope providers that offer services in the EU (including non-EU firms) to appoint an EU legal representative or designated establishment to receive and comply with orders by 18 August 2026; it sets basic enforcement/coordination rules and dovetails with GDPR, LED and e-Privacy. The e-Evidence package, therefore, expands cross-border access to stored data for criminal proceedings - a surveillance-adjacent power - but it does so within a framework that seeks to bake in judicial control, data-category tiers, short retention of preserved data, notification, and fundamental-rights safeguards, rather than authorising bulk or real-time monitoring.

Jurisprudence

From its earliest surveillance judgments to the latest rulings on bulk interception and encryption, the European Court of Human Rights has built a sequential body of [case law](#) under Article 8 ECHR that tightens legality, foreseeability, and proportionality requirements. In *Klass and Others v. Germany* (App. no. 5029/71, 1978), the Court accepted secret surveillance in principle but held that even the "menace

of surveillance” can be an interference, which must be strictly necessary and accompanied by effective oversight, planting the seed for later safeguards. In *Malone v. the United Kingdom* (App. no. 8691/79, 1984) the UK was found in breach because interception powers were not “in accordance with the law” - the rules lacked accessibility and foreseeability - establishing the [modern legality test](#). In *twin French cases* *Kruslin v. France* (App. no. 11801/85, 1990) and *Huvig v. France* (App. no. 11105/84, 1990) the Court condemned vague tapping regimes and insisted on precise statutory limits, record-keeping and supervision. It soon extended protection to the workplace and privileged communications: *Halford v. the United Kingdom* (App. no. 20605/92, 1997) held that intercepting a senior police officer’s office calls without a clear legal basis violated Article 8, recognizing a reasonable expectation of privacy at work, while *Kopp v. Switzerland* (App. no. 23224/94, 1998) underscored heightened safeguards where attorney-client communications may be affected. In *Amann v. Switzerland* (App. no. 27798/95, Grand Chamber, 2000) and *Rotaru v. Romania* (App. no. 28341/95, Grand Chamber, 2000) the Court faulted interception and secret-file practices for lacking sufficiently clear legal bases and effective remedies, broadening surveillance scrutiny to data storage and intelligence files. As digital tools spread, the Court refined minimum safeguards. *Weber and Saravia v. Germany* (dec., App. no. 54934/00, 2006), while declaring the application inadmissible, set out the six safeguards for strategic interception (clear scope, categories of people/communications, time limits, procedures for examining/using/retaining data, precautions in sharing, and supervision), which later cases repeatedly cite. It also policed employer monitoring and legacy regimes: *Copland v. the United Kingdom* (App. no. 62617/00, 2007) condemned covert monitoring of an employee’s phone, email and internet use; *Liberty and Others v. the United Kingdom* (App. no. 58243/00, 2008) found the UK’s then-interception framework insufficiently foreseeable; and *S. and Marper v. the United Kingdom* (App. nos. 30562/04 & 30566/04, 2008) invalidated indefinite retention of DNA/fingerprints of non-convicted persons. Turning to modern surveillance statutes and techniques, *Kennedy v. the United Kingdom* (App. no. 26839/05, 2010) tested the RIPA framework and, while finding no violation, emphasized independent oversight and remedies; *Uzun v. Germany* (App. no. 35623/05, 2010) accepted targeted GPS tracking as compatible with Article 8 when strictly necessary and proportionate; and *R.E. v. the United Kingdom* (App. no. 62498/11, 2015) insisted on especially robust safeguards for surveillance of lawyer–client consultations. The Grand Chamber’s *Roman Zakharov v. Russia* (App. no. 47143/06, 2015) became a watershed, since even absent proof of being personally tapped, the Court found Russia’s SORM regime structurally defective (over-broad purposes, weak prior authorisation, scant oversight, no notification), thus violating Article 8. Subsequent judgments tightened national-security surveillance: *Szabó and Vissy v. Hungary* (App. no. 37138/14, 2016) struck down anti-terror tapping powers for lacking judicial control and precise limits; *Benedik v. Slovenia* (App. no. 62357/14, 2018) held that identifying a user behind a dynamic IP address engages Article 8 and generally requires prior judicial authorisation. In *Big Brother Watch and Others v. the United Kingdom* (Grand Chamber, App. nos. 58170/13, 62322/14 & 24960/15, 2021) and the paired *Centrum för Rättvisa v. Sweden* (Grand Chamber, App. no. 35252/08, 2021) the Court accepted that bulk interception is not per se incompatible with the Convention, but found violations because the regimes lacked “end-to-end” safeguards - including prior independent authorisation of selectors/search terms, rigorous supervision, source/journalist protections, and strict data handling - thus recalibrating the standard for bulk signals intelligence. It then applied those requirements to other states in *Ekimdzhiev and Others v. Bulgaria* (App. no. 70078/12, 2022), finding inadequate legal safeguards and oversight, and, most recently, protected end-to-end encryption in *Podchasov v. Russia* (App. no. 33696/19, 2024), holding that compelled decryption orders that effectively require weakening encryption violate Article 8.

Read chronologically, Strasbourg case law moves from early legality and foreseeability (Malone; Kruslin/Huvig) to thicker procedural architectures (Weber and Saravia's six safeguards; Halford/Kopp on workplace and privilege; Amann/Rotaru on data files and remedies), then to technology-specific proportionality (GPS tracking in Uzun; dynamic IPs in Benedik; privileged consultations in R.E.). The Grand Chamber's turn in Zakharov constitutionalized systemic review of surveillance frameworks even without individualized victim proof, enabling structural challenges to laws themselves. With Big Brother Watch and Centrum for Rättvisa, the Court did not ban bulk regimes but clearly set conditions - prior independent authorisation of selectors, targeting and filtering limits, independent oversight, journalist/source protections, retention minimisation, and ex post notification where feasible - requiring an "end-to-end" chain of safeguards. Subsequent cases (Ekimdzhiev) show those standards travelling beyond the UK/Sweden. Finally, Podchasov updates the doctrine for the encryption era: protecting E2EE as a cornerstone of private communications and warning that backdoors or key-escrow mandates are incompatible with Article 8 because they expose everyone's communications to risk. These decisions map a clear trajectory: surveillance powers must be precisely framed in law, narrowly necessary, and embedded in independent, reviewable, end-to-end safeguards that adapt to evolving technologies rather than eroding baseline rights.

In addition to the human rights cases, jurisprudence from the Court of Justice of the European Union (CJEU) is also relevant to the issue of digital surveillance. CJEU is the EU's highest court and judicial authority, ensuring that European law is interpreted and applied uniformly across all member states and that EU institutions and Member States comply with their legal obligations.

Beginning with *Digital Rights Ireland and Seitlinger (Joined Cases C-293/12 & C-594/12, 8 Apr 2014)*, the Court of Justice invalidated the EU Data Retention Directive because blanket, undifferentiated retention of everyone's traffic/location data - without tight limits, prior review, or effective safeguards - was not "strictly necessary," setting the [modern baseline](#) that general and indiscriminate retention breaches the Charter (Arts 7 and 8). A year later, *Schrems (Safe Harbor) (C-362/14, 6 Oct 2015)* tied surveillance abroad to EU standards at home, striking down the EU-US Safe Harbor for failing to protect EU data against U.S. intelligence access and to provide redress, a move that made [third-country surveillance](#) an EU law problem, not just a foreign policy issue. In *Tele2 Sverige/Watson (Joined Cases C-203/15 & C-698/15, 21 Dec 2016)*, the Court translated *Digital Rights Ireland* into national practice. [Member States](#) cannot impose general and indiscriminate retention on providers; any retention must be targeted (e.g., by time, place, categories of persons) and access must be limited to serious crime, subject to prior review by a court or independent authority, with robust security and oversight. [Opinion 1/15 \(EU-Canada PNR\) \(26 Jul 2017\)](#) then warned that large-scale passenger-data transfers require strict necessity, tight retention, independent control, and sensitive-data safeguards, anticipating later "bulk use" rulings. In [Ministerio Fiscal \(C-207/16, 2 Oct 2018\)](#) the Court nuanced the access threshold: obtaining subscriber identity data (e.g., to link a SIM to a person) is a less serious interference that may be allowed for investigating ordinary crime, whereas access to traffic/location data still demands the "serious crime" and prior-review standard. *Schrems II (Privacy Shield) (C-311/18, 16 Jul 2020)* again linked surveillance to adequacy; it invalidated Privacy Shield because U.S. signals intelligence and redress mechanisms failed Charter tests; Standard Contractual Clauses survived but require case-by-case

assessments and [supplementary measures](#) where third-country surveillance looms. The Court then addressed national-security claims head-on in *Privacy International* (C-623/17, 6 Oct 2020) and *La Quadrature du Net and Others* (Joined Cases C-511/18, C-512/18 & C-520/18, 6 Oct 2020) it held that the ePrivacy regime applies even when states invoke national security, precluding general and indiscriminate retention or bulk transmission of provider data to security agencies; only strictly [limited measures](#) are possible (e.g., time-limited retention where there is a serious, genuine and present or foreseeable threat to national security; targeted retention; expedited preservation; and, subject to safeguards, generalized retention of IP addresses or civil identity data for specific aims). In *H.K. v Prokuratuur* (C-746/18, 2 Mar 2021) the [Court added](#) that prosecutors are not sufficiently independent to authorise access to retained communications data; prior control must be by a court or independent administrative body, and access must be confined to serious crime. *G.D. v Commissioner of the Garda Síochána* (C-140/20, 5 Apr 2022) reaffirmed these limits, rejected attempts to temporally limit the invalidity of incompatible national laws, and reiterated the strict [conditions for retention and access](#) under Articles 7 and 8 of the Charter. In the PNR field, *Ligue des droits humains* (C-817/19, 21 Jun 2022) preserved the core of the PNR Directive but only via a Charter-compliant narrowing: automated risk-assessment models must be genuinely necessary and proportionate, retention must be constrained, and [intra-EU extension](#) demands strict justification and safeguards. The Court applied and refined its template in *SpaceNet & Telekom Deutschland* (Joined Cases C-793/19 & C-794/19, 20 Sep 2022), again barring general retention but allowing general IP-address retention for serious crime and targeted/time-limited retention tied to concrete threats, together with [VD and SR](#) (Joined Cases C-339/20 & C-397/20, 20 Sep 2022), which exported those standards to market-abuse investigations and forbade courts from shielding unlawful regimes by limiting the effects of invalidity.

Taken together, these rulings chart a coherent system: (i) no blanket data hoarding (*Digital Rights Ireland* and *Tele2/Watson* kill indiscriminate retention), then the Court resists national-security workarounds in *Privacy International* and *La Quadrature* by demanding end-to-end safeguards (strict necessity; limited purposes; short retention; strong oversight; prior independent review; auditability; and, where feasible, ex-post notification); (ii) calibrated access thresholds (*Ministerio Fiscal* recognizes lower-intensity identity lookups, while *Prokuratuur* and *G.D.* insist that access to traffic/location data be reserved for serious crime and authorised by a truly independent body); (iii) extraterritoriality (*Schrems I/II* make third-country surveillance decisive for cross-border transfers); and (iv) sectoral extensions under constraint (*Ligue des droits humains* keeps large-scale PNR use on a tight leash, and *SpaceNet/Telekom* plus *VD & SR* confirm narrowly-tailored exceptions (e.g., IP-address retention, expedited preservation, geographic/time targeting) without reopening the door to generalised surveillance. In short, CJEU jurisprudence permits targeted, threat-led, reviewable surveillance while rejecting indiscriminate regimes, binding Member States and shaping EU-external data flows alike.

3.3 Inter-American Human Rights Standards

The Inter-American Human Rights System has also developed clear standards on digital surveillance, grounded in the American Convention on Human Rights (ACHR) and jurisprudence of the Inter-American Court of Human Rights (IACtHR) and Inter-American Commission on Human Rights (IACHR).

At the foundation of the Inter-American system's approach to digital surveillance are the rights guaranteed under the ACHR. Article 11 enshrines the right to privacy, honour, and dignity, protecting individuals against arbitrary or abusive interference with their private life, family, home, and communications. This provision has been interpreted to cover not only physical spaces but also digital and online interactions. Article 13 safeguards freedom of expression, which encompasses the right to seek, receive, and impart information of all kinds, a right that can be undermined when surveillance produces self-censorship or fear of state monitoring. Finally, Article 8 guarantees due process and fair trial rights, which are directly engaged when surveillance is used as part of investigations or prosecutions, requiring that any such measures respect legality, transparency, and procedural fairness. Together, these articles establish a normative baseline in which digital surveillance is not prohibited outright but is permissible only if it respects privacy, does not unduly restrict freedom of expression, and is subject to rigorous procedural safeguards to protect individuals from abuse.

The IACtHR has developed key jurisprudence on surveillance, most prominently in [Escher et al. v. Brazil \(2009\)](#), which remains the cornerstone ruling on digital privacy in the region. In this case, Brazilian authorities had intercepted and disclosed telephone communications of members of a rural workers' association without adequate legal basis or safeguards. The Court held that such interceptions violated Articles 11 and 13 of the ACHR, stressing that any restriction on the right to privacy or freedom of expression through surveillance must satisfy four cumulative conditions: it must be expressly provided by law, pursue a legitimate aim consistent with the Convention (such as national security or protection of rights), be necessary and proportionate in a democratic society, and be subject to independent judicial authorization and oversight. Beyond *Escher*, the Court has reinforced these principles in its Advisory Opinions. In [OC-5/85 on compulsory association](#), it underscored that restrictions on expression must always pass a strict proportionality test, a standard later applied to the surveillance context. More recently, in [OC-23/17 on the environment and human rights](#), the Court highlighted the centrality of access to and control over information in protecting rights, which extends to protecting individuals from unjustified intrusions into their communications and data. These rulings and opinions firmly establish that under the Inter-American system, digital surveillance is only legitimate when it is lawful, necessary, proportionate, and overseen by an independent authority, and that indiscriminate or uncontrolled surveillance is incompatible with democratic values and the Convention framework.

The IACHR has complemented the Court's jurisprudence by elaborating detailed standards on surveillance in its thematic reports, in particular those prepared by the Office of the Special Rapporteur for Freedom of Expression. In its [2013 Report on Freedom of Expression and the Internet](#), the Commission made clear that mass or indiscriminate surveillance is incompatible with the American Convention, as it inherently undermines both privacy and freedom of expression by creating a climate of self-censorship. It emphasized that surveillance measures must always be targeted, exceptional, and subject to strict oversight by an independent authority. Building on this, the 2015 the Special Rapporteur annual report underscored that surveillance programs must pass the three-part test of legality, necessity, and proportionality, and that laws authorizing such practices must be clear, accessible, and precise. The [report](#) also stressed the need for prior judicial authorization, independent monitoring, and effective remedies for individuals affected by abusive surveillance. In 2017, in its report *Standards for a Free, Open and Inclusive Internet*, the Commission explicitly rejected the legitimacy of blanket or indiscriminate data collection, stating that such practices "cannot be reconciled with the inter-American human rights framework." Instead, States were urged to [adopt laws](#) that prevent arbitrary surveillance,

establish robust data protection frameworks, and guarantee transparency and accountability mechanisms. The Commission's reports build a strong normative framework, condemning mass surveillance, demanding strict legal and procedural safeguards, and highlighting the chilling effect that unchecked surveillance has on democratic debate and human rights in the digital age.

African Regional Standards on Digital Surveillance

Continental Legal and Policy Standards on Surveillance

The African Charter on Human and Peoples' Rights (1981) underpins Africa's human rights system. While the Charter does not explicitly list a right to privacy, the African Commission on Human and Peoples' Rights has recognized that privacy is implied by other rights, such as the rights to dignity and integrity of the person. Unlawful interference with personal privacy is seen as violating the Charter's protection of human dignity. This provides [a basis for African institutions](#) to develop standards against digital surveillance despite the Charter's silence on privacy. Over the past decade, African continental bodies have indeed articulated clear norms to [regulate state surveillance](#) in the digital realm.

A landmark soft-law instrument is the [Declaration of Principles on Freedom of Expression and Access to Information in Africa](#) (2019), adopted by the African Commission. This Declaration dedicates Principle 41 to privacy and communications surveillance. It categorically prohibits indiscriminate or untargeted surveillance of people's communications, effectively banning mass surveillance by states. Targeted surveillance is permitted only under strict conditions: it must be authorized by law, serve a legitimate aim (such as investigating serious crime), comply with international human rights standards, and be based on reasonable suspicion. The Declaration further requires that any law permitting targeted surveillance include robust safeguards for privacy. Such safeguards include: prior independent judicial authorization for surveillance, due process, limitations on the duration and scope of surveillance, notification of the person after surveillance (within a reasonable time), transparency about the use of surveillance powers, and oversight by an independent supervisory body. These [principles](#) set a clear continental standard that mirrors global privacy norms, namely, no mass surveillance and only strictly regulated targeted interception of communications in line with necessity and proportionality.

The African Commission has reinforced these standards through [official resolutions](#). Notably, in 2016 it affirmed that the "same rights that people have offline should be protected online," implicitly recognizing privacy in digital spaces. More recently, at its 77th Session in November 2023, the Commission adopted Resolution 573 on "the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa." In this [resolution](#), the Commission expresses deep concern about the "prevalence of mass surveillance and unlawful targeted communication surveillance" in Africa and the lack of adequate privacy frameworks in many states. It condemns indiscriminate surveillance as incompatible with human rights, noting the disproportionate targeting of journalists, human rights defenders, civil society and opposition figures by such measures. The Commission calls on States to align their surveillance laws with international human rights standards, specifically by incorporating safeguards like independent judicial authorization and effective oversight mechanisms. It urges that states "only engage in targeted communication surveillance that is authorized by law, conforms with international human rights standards, and is premised on reasonable suspicion that a serious crime has been or is being carried out". The 2023 resolution even goes further to encourage use of privacy-protecting technologies (and warns against undermining encryption), and it demands that victims of illegal surveillance have access to effective remedies in court. The Commission's resolutions,

while not binding, carry normative force: they clearly establish a continental prohibition on mass surveillance and insist on stringent conditions for any permitted surveillance (legality, necessity, proportionality, oversight, transparency, and remedy).

At the treaty level, the African Union has also set standards that indirectly constrain digital surveillance. The [AU Convention on Cyber Security and Personal Data Protection](#) (adopted 2014, known as the Malabo Convention) is the first binding African treaty on data privacy. It finally entered into force in 2023, making it the only binding [regional data protection treaty](#) outside Europe. The Malabo Convention obliges States to establish robust legal frameworks to protect personal data privacy in the digital age. Its preamble and text affirm that the right to privacy is grounded in African and international human rights law. The Convention creates a continent-wide framework for data protection, requiring states to adopt legislation and institutions to prevent the misuse of personal information. For example, it mandates independent data protection authorities and grants individuals enforceable rights over their data (such as the right to be informed of data collection, to access their data, to object to processing, and to request deletion). These provisions directly limit surveillance abuses by imposing data privacy obligations on governments. Under Malabo, any surveillance involving the collection, storage or sharing of personal data must comply with principles of lawful, fair, and necessary processing and respect the rights of data subjects. Overall, the Malabo Convention seeks to balance state security prerogatives with individuals' fundamental privacy rights, requiring that even in the pursuit of cybersecurity or crime prevention, [personal data](#) is handled in line with human rights standards. Once implemented into national laws, these requirements should constrain blanket digital surveillance and ensure oversight of intelligence data processing.

Beyond the continental level, Africa's sub-regional organizations have also advanced privacy norms relevant to surveillance. In West Africa, for instance, ECOWAS adopted a binding [Supplementary Act on Personal Data Protection \(2010\)](#) that requires all member states to pass privacy laws and establish data protection authorities. This ECOWAS Act explicitly aims to protect the privacy of individuals' data during its collection, storage, and use (which would include data obtained through surveillance) and to ensure such processing is governed by law. In Southern Africa, the [SADC published a Model Law on Data Protection \(2013\)](#) to guide countries in enacting privacy legislation. Similarly, the East African Community and the African Union have developed [model laws or policy frameworks](#) on cybersecurity and data privacy. All these instruments strengthen the legal infrastructure guarding against unchecked surveillance, by asserting that personal information (including communications data) must be collected and used only for legitimate purposes and with respect for privacy rights.

It is also worth noting the [role of African civil society](#) and multi-stakeholder initiatives in setting surveillance norms. The African Declaration on Internet Rights and Freedoms (2014), while not an official AU document, has been endorsed by numerous African organizations and even referenced by African Commission officials. This Declaration explicitly addresses surveillance, stating that mass or indiscriminate surveillance is a "disproportionate interference" with rights and should be "prohibited by law." It affirms that intercepting or monitoring digital communications interferes with the rights to privacy and freedom of expression, "whether or not the data is subsequently examined or used." Echoing the African Commission's stance, the civil society declaration insists that any targeted surveillance must be lawful, necessary and proportionate, and it lays out minimum principles: surveillance should be authorized by an impartial court, used only when there is reasonable suspicion of serious crime, limited in scope and time, overseen by parliament or other independent bodies, and with users being notified of surveillance after the fact. These principles have influenced discourse and even the wording of the African Commission's own guidelines (indeed, the Commission's 2019 Declaration and the 2023 Resolution align closely with these tenets).

Emerging African standards on digital surveillance in summary:

- **No Mass Surveillance:** Blanket, indiscriminate surveillance of citizens' communications (e.g. bulk interception of phone or internet data without targeting) is not permissible under [African human rights standards](#). African bodies have labeled [mass surveillance as a violation](#) of the right to privacy and other freedoms, given its disproportionate impact. States should refrain from any surveillance practice that is not selective and law-based.
- **Strict Necessity and Legality for Targeted Surveillance:** Targeted surveillance (such as wiretaps, hacking, or monitoring of specific individuals) is allowed only if authorized by law and strictly necessary for a [legitimate aim](#) like combatting serious crime or terrorism. Any [surveillance measure](#) must be proportionate, i.e. carefully limited in scope and duration to what is needed for that aim. Vague or overbroad surveillance powers violate these standards. African instruments demand that surveillance laws themselves be clear and [accessible](#) to the public (no secret laws), so people know how their privacy might be affected.
- **Judicial and Independent Oversight:** Surveillance should never be at the sole discretion of security agencies or the executive. [African standards](#) require independent oversight at multiple stages. Prior review and approval by an impartial judge or court is *essential* before communications surveillance is conducted. After approval, the [implementation](#) of surveillance should be subject to continuous monitoring and periodic review by independent oversight bodies (e.g. privacy commissioners or legislative committees) to prevent abuse. The African Commission has highlighted the need for "effective monitoring and regular review by independent oversight mechanisms" as a safeguard.
- **Transparency and User Notification:** Consistent with international best practice, African soft law calls for as much transparency as possible around surveillance. This includes post-surveillance notification to individuals. The [African Declaration and the Commission's Principles](#) both stipulate that individuals who were surveilled should be informed of that fact within a reasonable time after the surveillance ends, so long as notifying them will not defeat the purpose of the investigation. States are also encouraged to publish information on the nature and scope of surveillance (e.g. aggregated data on how often it is used). Such transparency allows the public and civil society to hold authorities accountable.
- **Data Protection and Storage:** A recurring theme is that personal data collected through surveillance must be protected. The Commission's Declaration (Principle 42) and the [AU's Malabo Convention](#) both demand that personal information be handled lawfully and securely. Data obtained for [one legitimate purpose](#) (e.g. a terrorism investigation) should not be misused for unrelated purposes. It should also not be retained longer than necessary. The AU data protection regime compels states to establish rules on data retention, sharing, and deletion that guard against abuse. This means surveillance databases should not become an open-ended repository

of citizens' data – there must be limits and protections in place in line with the right to privacy.

- **Encryption and Digital Security:** Although not directly about state surveillance, another emerging standard is that governments should not undermine encryption or other privacy-enhancing technologies. In its 2023 Resolution, the [African Commission](#) specifically urged states to desist from laws or measures that weaken encryption (such as requiring “backdoors” into encrypted services), unless such measures are demonstrably justified in line with human rights law. This stance recognizes that strong encryption is often a safeguard against unlawful surveillance and a protector of privacy in the digital age.
- **Remedies for Violations:** African standards emphasize that when surveillance oversteps legal bounds, individuals must have redress. The African Commission explicitly calls on states to ensure that [“victims of violations arising from arbitrary surveillance measures have access to effective remedies”](#). This entails having avenues to challenge illegal surveillance in court, seek damages, or demand deletion of unlawfully collected data. States are also urged to investigate and punish officials who conduct illegal or indiscriminate surveillance. The principle of accountability is thus ingrained: surveillance operations should not be above the law, and those affected by privacy breaches deserve justice.

Case Law and Jurisprudence on Surveillance in Africa

The African Commission on Human and Peoples' Rights has addressed aspects of privacy and surveillance in its case decisions, although somewhat indirectly. Because the African Charter does not explicitly guarantee a right to privacy, individuals have typically brought surveillance-related complaints under other rights (such as freedom of expression, freedom of association, or the right to a fair trial). The [Commission](#) has shown willingness to consider these complaints, often reading privacy considerations into the broader rights and principles of the Charter. In its 2015 Principles on Countering Terrorism, for example, the Commission itself noted that various Charter rights (like Articles 8, 10, 11, 12, 14, and 18) imply a sphere of personal life free from state interference. This means that surveillance which intrudes on one's home, communications or family life can violate the [Charter's protections of personal integrity](#), even if “privacy” is not named outright.

One of the few decided cases touching on surveillance is *Lawyers for Human Rights (Swaziland) v. Swaziland (Communication 251/2002)*. [This complaint](#) challenged a 1973 State of Emergency proclamation and a 2001 decree in the Kingdom of Swaziland (now Eswatini). Under the King's 1973 Proclamation, the constitution's Bill of Rights was suspended, political parties were banned and the King assumed all legislative, executive, and judicial powers. The decree of 2001 further ousted the jurisdiction of courts in certain cases (removing checks on the executive). These measures created a regime of unchecked state power, under which security forces could surveil and suppress dissent without legal restraint. The complainant alleged numerous human rights violations, including the rights to free expression, association, and a fair trial. In its 2005 decision, the African Commission found Swaziland in breach of several Charter provisions. It held that the sweeping powers asserted by the government (including the ban on political activity and the override of normal judicial process) violated the Charter's Article 7 (right to fair trial), Article 10 (freedom of association), Article 11 (freedom of assembly),

Article 13 (right to participate in government), as well as the duty to uphold Charter rights in domestic law (Article 1) and to ensure an independent judiciary (Article 26). Although the Commission's decision did not explicitly mention a "right to privacy," the implication is that surveillance and other coercive measures taken under the state of emergency were part of the unlawful restrictions. By abolishing judicial oversight and democratic safeguards, the Swazi authorities had free rein to monitor communications, search homes, or detain opponents arbitrarily. The Commission's ruling condemned this unchecked surveillance state and recommended that Swaziland repeal or amend the offending laws to conform with the Charter. The *Lawyers for Human Rights* case thus illustrates how the Commission will intervene when surveillance powers, especially those imposed under the guise of national security, undermine the fundamental freedoms of expression, association, and the rule of law.

It must be noted that explicit case law on digital surveillance in the African system remains limited. Aside from the above and a handful of older cases dealing with state security laws, individuals have rarely brought pure "right to privacy" claims to the African Commission or the African Court on Human and Peoples' Rights. This is partly due to the Charter's lack of a standalone privacy clause, and partly because many surveillance disputes may be addressed at the national level first. However, the normative guidance from the Commission is clear, and we may see more cases in the future invoking these standards. In fact, [the African Commission's recent Resolution 573 \(2023\)](#) explicitly "recogniz[es] the lack of adequate national frameworks on privacy [and] communication surveillance" in Africa and urges states to fill that gap. The resolution calls for states to not only reform their laws but also to "investigate and prosecute" abuses of surveillance powers and to ensure victims have access to justice. This emphasis on accountability lays a possible foundation for future litigation: individuals whose rights are violated by unlawful digital surveillance should be able to seek remedies, either in domestic courts or, if those fail, through the African Commission or African Court.

The African Court on Human and Peoples' Rights, since it began operating in 2006, has not yet had a landmark case purely on digital surveillance or the right to privacy. Many state parties have not allowed direct individual access to the Court, which limits the cases reaching it. Nonetheless, the Court could hear such a case under its mandate to interpret the Charter and other human rights instruments.

In the absence of African Court judgments on surveillance to date, much of the regional judicial insight comes from national courts and sub-regional courts. For example, in 2019 the Constitutional Court of South Africa (a domestic court) delivered a pivotal ruling in the [AmaBhungane v. Minister of Justice](#) case, striking down parts of a surveillance law (the RICA Act) for failing to meet constitutional privacy standards. The South African court ruled that secret bulk interception and the lack of post-surveillance notification were unconstitutional, and it read in requirements for judicial warrants and for notifying surveillance subjects after an investigation ends. These requirements closely mirror the African Commission's recommendations (judicial oversight, transparency, etc.), showing how domestic jurisprudence is aligning with regional human rights principles. Likewise, the ECOWAS Community Court of Justice in recent years has handled cases on digital rights (for instance, challenging internet shutdowns and privacy violations), applying the African Charter and international law to find violations. While many cases have focused heavily on freedom of expression and access to information, the broader issue of digital rights also implicitly covers privacy concerns, such as freedom from arbitrary surveillance and data protection. The [Ogwuche v. Federal Republic of Nigeria](#) case, for example, involved the court examining restrictions on media programs and whether they were justified, touching upon state power over communications. Such developments at the national and sub-regional levels contribute to an evolving body of African jurisprudence affirming the right to privacy in the digital age.

Chapter 4. A failing system? Legal trends and gaps

This chapter considers the legal frameworks governing digital surveillance in India, Pakistan, Kenya, Italy, Serbia, Brazil, Mexico, El Salvador, Lebanon and Jordan (as presented in summary above and in detail in Part 2), highlighting how each country balances state surveillance powers with safeguards for privacy and press freedom. It focuses on six key dimensions: (1) judicial safeguards and due process (e.g. warrant requirements and judicial oversight), (2) legal limits on surveillance (necessity, proportionality, and targeted vs. mass surveillance), (3) oversight and accountability mechanisms (independent regulators, legislative controls), (4) remedies and redress available to individuals, (5) distinctions between general surveillance frameworks vs. spyware-specific rules, and (6) broader regional or systemic patterns.

The analysis reveals emerging patterns, notable contrasts, and persistent regulatory gaps across these diverse jurisdictions, drawing on constitutional norms, statutory laws, and recent case developments.

4.1 Judicial Safeguards and Due Process Requirements

A strong judicial role in authorizing surveillance is a common thread in the formal laws, reflecting the principle that interceptions of private communications should occur only with prior court approval and due process. Most of these nations enshrine privacy or secrecy of communications as a fundamental right in their constitutions, only to be limited by law and typically by judicial warrant. For example:

- Italy's Constitution (Art. 15) declares communications inviolable and allows restrictions "only by judicial authority and under guarantees of law", setting a strict baseline of independent oversight. Italy's criminal procedure code accordingly requires a judge's authorization for any interception, confined to specified serious crimes.
- Brazil's 1988 Constitution similarly guarantees privacy of communications and permits intrusions solely with a judicial order for criminal investigations. Brazil's dedicated Interception Law (1996) mandates that a judge approve all wiretaps, typically for an initial 15-day period, with prosecutors demonstrating necessity before renewal.
- Mexico's Constitution (Art. 16) enshrines the inviolability of private communications; any interception or access to communications data requires a prior judicial warrant based on a legitimate aim. This principle underpins Mexico's telecommunications law, which reiterates that content interception demands a federal judge's authorization.
- El Salvador's Constitution (Art. 24) likewise prohibits any communication interception without a prior judicial warrant, providing a strong textual safeguard. In practice, El Salvador's Special Law for Telecommunications Intervention (LEIT, 2010) built on this by detailing warrant procedures for wiretaps in serious crimes, with judges centrally involved in approving and supervising interceptions.
- Serbia's Constitution (Art. 41) protects confidentiality of communication and permits surveillance only when "provided by law and subject to strict judicial control," a standard aligning with European human rights norms. Consequently, Serbia's Criminal Procedure Code

requires court orders for any interception, ensuring investigative surveillance remains bounded by necessity and judicial review.

- Kenya's 2010 Constitution (Art. 31) guarantees the right to privacy in one's communications, allowing infringements only with "lawful justification" in a manner reasonable and justifiable in an open, democratic society. Kenya's statutes reflect this: the National Intelligence Service Act and Prevention of Terrorism Act authorize communication monitoring only with a High Court warrant, directly embedding judicial authorization into national security surveillance.
- Pakistan's Constitution (Art. 14) affirms privacy as inviolable, a right the Supreme Court has interpreted to extend beyond the home into public and digital realms. In a landmark 1990s ruling, Pakistan's top court held that unauthorized phone tapping violates constitutional privacy and dignity, underscoring that surveillance must have legal sanction and due process. Statutorily, Pakistan's Investigation for Fair Trial Act 2013 introduced a warrant-based system for electronic interception by requiring a judicial warrant upon "reasonable belief" of involvement in serious crime, though tellingly no warrants were issued under this framework for many years (suggesting either infrequent use or reliance on extra-legal methods).
- Lebanon's Law 140/1999 on communications secrecy was pioneering in the Arab world for codifying surveillance procedures. It sets up two tracks: judicial warrants for criminal investigations, which must specify the targeted line, offense, and a max duration of two months, and "exceptional" administrative authorizations by the Interior or Defence Minister (with Prime Minister's consent) for national security or terrorism cases. Even the latter requires ex post verification by a special high-level judicial commission. On paper, this embeds classic rule-of-law controls - prior written authorizations, defined scope, and time limits - into Lebanon's surveillance regime.
- Jordan, notably, lacks a singular comprehensive surveillance statute or explicit constitutional clause on communication secrecy. In practice, broad national security laws and the powers of the intelligence services fill the gap. While nominally any interception should have legal basis and some form of permission, Jordanian law does not clearly mandate judicial warrants for surveillance, leaving a murky area governed by internal security practices and executive discretion. This absence of a codified warrant requirement stands in contrast to the other countries and reflects Jordan's heavy emphasis on security imperatives over individual due process in surveillance matters.

Across most of these jurisdictions the formal legal baseline is that digital surveillance must be conducted under judicial supervision. Constitutions and laws widely require a court-issued warrant or similar judicial order before authorities can intrude upon private communications. This is a critical due process safeguard, intended to prevent arbitrary or politically motivated monitoring. However, in practice, the strength of this safeguard varies greatly. In some countries, broad national security exceptions or emergency measures have been used to bypass judges (e.g. El Salvador's state of exception, or Jordan's security operations), and in others the warrant process exists on paper but is undermined by secret surveillance systems operating without court approval (e.g. Pakistan's recently exposed "LIMS" interception system). Nonetheless, the unifying principle of prior judicial authorization, at least as an ideal, runs through the legal frameworks, marking a key distinction between legitimate, rule-bound surveillance and unlawful snooping.

4.2 Legal limits on surveillance powers: proportionality, necessity, and scope

Countries researched for this report impose some legal limits on surveillance powers, often invoking principles of necessity, proportionality, and specificity to confine how, when, and against whom surveillance may be conducted. The letter of the law generally favours targeted surveillance (focused on specific suspects or threats) over indiscriminate collection, though the breadth of actual practices can diverge from these ideals. Key limitations include:

- **Necessity and proportionality tests:** Many frameworks explicitly require that any infringement of privacy serves a legitimate aim and is necessary and proportionate to that aim. In India, for instance, the Supreme Court's landmark *Puttaswamy* judgment (2017) elevated privacy to a fundamental right and held that any surveillance measure must satisfy "legality, necessity, and proportionality," using the least intrusive means available. Kenya's Constitution demands that even legally authorized searches or monitoring be reasonable and justifiable in an open democratic society, effectively a proportionality standard for surveillance powers. Italy and Serbia, influenced by European human rights jurisprudence, similarly embed proportionality. Italy's courts and data protection authority have insisted that surveillance tools (from wiretaps to CCTV) be narrowly tailored and used only when appropriate. Serbian law requires that investigative surveillance occur "within the boundaries of necessity and proportionality", aligning with EU standards and aiming to prevent abuse or overreach. In practice, these tests mean surveillance should be a last resort, employed only for sufficiently serious concerns and in a manner that minimizes collateral intrusion on privacy.
- **Scope limits – targeted vs. mass surveillance:** On paper, all ten countries favour targeted surveillance (individualized interception) and either prohibit or tightly restrict mass, bulk surveillance. Typically, surveillance laws enumerate specific grounds or offenses that can justify interception (e.g. serious crimes, threats to national security) and often require identifying the particular person, device, or communication line to be monitored. Time limits on interception warrants are common: Brazil's law limits intercept orders to 15 days (renewable); Lebanon's Law 140 caps authorizations at 2 months; El Salvador's LEIT allows initial surveillance periods with possible 72-hour extensions for new leads. These constraints are meant to prevent open-ended fishing expeditions. Several countries explicitly criminalize unauthorized surveillance to deter abuse: Kenya's cybercrimes law penalizes any interception conducted outside legal procedures, and Serbia's criminal code likewise bans the unlawful collection of personal data, reinforcing that only duly authorized surveillance is lawful.

Despite these formal limits, pressures to engage in broader surveillance have tested legal boundaries. In practice, some governments have pushed for or implemented mass surveillance-like measures, often justified by national security or public safety, sometimes in tension with necessity and proportionality principles:

- *Bulk data retention:* A number of countries require telecommunications providers to retain large volumes of user data (metadata) for potential government access. For example, Mexico's 2014 telecom law mandates that providers keep call detail records and other metadata for 6 to 24 months and hand it over to law enforcement on a judge's

request. Serbia's Electronic Communications Law imposed blanket retention of traffic and location data for all users, creating a pool of data accessible to authorities via court order. These retention regimes, while intended to aid investigations, effectively amount to mass surveillance of the population's communications metadata. They have drawn criticism for their breadth; the EU Court of Justice's jurisprudence disallows indiscriminate, generalized data retention as disproportionate, a standard that casts doubt on Serbia's regime and similar laws elsewhere.

- *Emergency or national security overrides:* Several countries permit extraordinary surveillance powers during states of emergency or for national security threats, which can become de facto mass surveillance if not narrowly applied. In El Salvador, for example, a "State of Exception" declared in 2022 amid gang violence temporarily suspended the normal warrant requirement and enabled authorities to monitor communications with almost no judicial oversight. This led to expansive surveillance and mass arrests, alarming human rights observers. Pakistan's colonial-era Telegraph Act (1885) and Official Secrets Act (1923) also provide broad emergency interception powers ("in the interest of public safety" or during "public emergency"), language vague enough to allow wide surveillance if invoked. Such provisions risk being used as catch-alls to justify surveillance without individualized suspicion, unless strictly confined.
- *Expansion in practice:* In some cases, authorities have simply exceeded legal limits in practice. A striking example is Lebanon between 2012 and 2014, when security agencies, citing terrorism concerns, sought and obtained blanket access to telecom data, including countrywide records of SMS, internet sessions, and subscriber information, far beyond the two-month targeted intercepts envisaged by Law 140/1999. Lebanese officials repeatedly issued Cabinet decrees granting unrestricted, bulk access to all telecommunications data for months at a time, an approach Lebanese jurists warned "violated Law 140 and far exceeded its targeted design". This marked a clear pivot toward mass surveillance, essentially irrespective of individualized warrants, in contravention of the law's proportionality safeguards. Similarly, Pakistan's secret rollout of a "Lawful Intercept Management System (LIMS)" in telecom networks enabled intelligence agencies to directly tap into carriers' data streams, extracting voice, SMS, and internet traffic in real time without any case-by-case review. When details of LIMS surfaced during a court case in 2024, it became evident that this system permitted mass, automated access to users' communications, bypassing the judicial warrant process entirely. The Islamabad High Court considered this unwarranted surveillance as unlawful and briefly barred its use, though the intervention was later stayed on jurisdictional grounds. These incidents reveal a gap between the targeted surveillance model on the books and the broader surveillance appetite of security agencies in practice.
- **Judicial enforcement of limits:** Courts in several countries have stepped in to enforce proportionality and quash overly broad surveillance measures. In Brazil, the Supreme Federal Court in 2020 struck down a government order that would have compelled telecom companies to turn over the personal data of every mobile phone user in the country to a statistics agency during the COVID-19 pandemic. The Court found this bulk data transfer lacked clear safeguards and violated constitutional privacy guarantees, emphasizing that "mass data collection without

individualized suspicion” is impermissible. Mexico’s Supreme Court similarly invalidated the 2021 plan to create a national mobile SIM user registry (PANAUT) with mandatory collection of all users’ biometric data, ruling in 2022 that such a sweeping database failed the necessity and proportionality tests and posed a disproportionate risk to privacy. Also in Kenya, courts have demanded procedural and impact reviews for new surveillance tools: the *Okiya Omtatah* cases in 2018 halted the rollout of a Device Management System (a network monitoring tool) due to privacy concerns and lack of public input, and later judgments required thorough data protection assessments before implementing biometric ID systems. These judicial actions underscore a trend, demonstrating that where robust independent courts exist, they increasingly insist on narrow tailoring and transparency for surveillance programs, reinforcing legal limits when legislatures or agencies overreach.

Overall, legal limits across these countries prioritize targeted, case-specific surveillance subject to tests of necessity and proportionality, at least as an ideal. Many laws explicitly ban fishing expeditions and mandate the destruction of collected data if not needed for prosecution. El Salvador’s LEIT even requires unused intercepted material to be destroyed after six months unless a judge orders otherwise. Yet, persistent gaps emerge in practice. Broad data retention laws and bulk collection exercises blur the line between targeted and mass surveillance, and vague national security exemptions can be stretched to justify near-limitless monitoring. The tension between formal legal restraints and security practices is evident in multiple countries. Where governance is stronger and courts are assertive (e.g. Italy, Brazil, Mexico, Kenya), there is pushback on disproportionate measures. Conversely, in more securitized or executive-dominated environments (Pakistan, Jordan, of late El Salvador), the trend is toward surveillance operations outpacing the strict letter of the law. This dichotomy highlights the importance of not just having legal limits on paper, but also of institutional checks to enforce those limits.

4.3 Oversight and accountability mechanisms

Effective oversight and accountability are crucial to ensure that surveillance powers are not abused. The countries covered by this report exhibit a spectrum of oversight frameworks, from robust, multi-layered controls in some democracies to minimal, opaque oversight in more authoritarian settings. Key oversight mechanisms include:

- **Independent data protection or privacy authorities:** Many nations have established independent regulators to oversee personal data handling, which indirectly or directly covers surveillance activities. For instance, Kenya’s Data Protection Act (2019) created the Office of the Data Protection Commissioner (ODPC), an independent regulator empowered to register data processors, investigate complaints, and issue penalties for privacy violations. Notably, the ODPC’s mandate extends to public bodies including security agencies when they process personal data, subject to national security exceptions, a provision already tested in Kenyan courts as they debate how far privacy oversight can intrude into surveillance agencies. Serbia’s Commissioner for Information of Public Importance and Personal Data Protection serves a similar role, with authority to probe government or private entities’ data practices, order compliance, and sanction violators. Brazil’s National Data Protection Authority (ANPD), provides oversight of personal data use across sectors, including by government bodies (though national security data is exempted), and can issue guidelines or fines to enforce compliance. Italy’s Garante (Data Protection Authority) predates many, and has actively shaped surveillance

practices by issuing guidelines (e.g. on video surveillance) emphasizing proportional use and data minimization. These authorities act as independent watchdogs over surveillance insofar as it involves personal data, offering a channel for complaints and an additional check beyond the courts.

- **Judicial and legislative oversight:** Judicial oversight is primarily through the warrant process and subsequent judicial review of surveillance conduct. However, some countries supplement this with specialized bodies or reporting requirements:
 - *Judicial commissions/boards:* Lebanon's Law 140 provides for a Verification Commission composed of top judges to review administrative interception decisions after the fact. Kenya's intelligence law set up an Intelligence Service Complaints Board where individuals can report abuses by the surveillance agency, a quasi-oversight body meant to address grievances outside the regular courts. In practice, the effectiveness of these bodies hinges on their independence and transparency. Lebanon's commission, for example, operates largely in secret, and while it has reportedly rejected some overly broad surveillance requests, its proceedings are opaque and rarely made public, contributing to an oversight gap for bulk surveillance actions.
 - *Parliamentary oversight and reporting:* Several democracies require the executive to keep the legislature informed about surveillance activities. Serbia's Electronic Communications Law mandates annual reports to Parliament on the number of data access requests made by authorities. This formal accountability to elected representatives is intended to prevent unchecked surveillance, though its impact depends on parliamentary will to scrutinize security services. Italy and Brazil have parliamentary committees that oversee their intelligence services, and Brazil's Congress has held inquiries into surveillance scandals (for instance, past legislative scrutiny of the NSA's activities in Brazil, and current debates prompted by spyware revelations). In Mexico, until recently, the autonomous transparency body INAI and congressional commissions both played roles in prying open information on surveillance operations, such as demanding disclosure of spyware contracts.
 - *Transparency and public accountability measures:* Legal requirements for transparency can indirectly serve as oversight. Mexico's transparency laws (2014–2016) obligated authorities to disclose information about their operations (with allowances for national security exemptions), and strengthened the National Transparency Institute (INAI) to enforce access to information. Through such mechanisms, journalists and civil society could request, for example, data on how often surveillance powers are used or details on procurement of spyware, adding public scrutiny. Mexican courts have upheld that even sensitive surveillance-related records (like Pegasus spyware purchase contracts) cannot be kept entirely secret; in 2024 the Supreme Court and lower courts ordered agencies to release redacted versions of Pegasus spyware documents in response to FOI requests, affirming that surveillance tech procurement is subject to public oversight and transparency rules. Kenya's 2021 Data Protection regulations similarly impose transparency obligations, requiring entities (potentially including security agencies) to

register and disclose high-risk data processing such as systematic monitoring, which can shine light on surveillance programs.

- **Institutional checks within government:** The design of some surveillance laws includes internal checks. For example, India's interception rules (Rule 419A of the Telegraph Rules) require that every interception order approved by the executive (typically by the Home Secretary) be reviewed by a Review Committee of senior officials to confirm it met legal standards. While this is not independent oversight in the strict sense (since it's still within the executive branch), it is a procedural accountability step. Similarly, in Lebanon, the requirement that the Prime Minister and a panel of ministers sign off on national security intercepts adds a degree of collective responsibility at the highest level. Italy's system keeps judicial control front and centre (with investigating judges closely supervising intercept execution and storage of intercept material), and its laws mandate strict record-keeping and eventual destruction of intercept data if not used, subject to a judge's oversight, which creates an audit trail and prevents indefinite secret archives.

Despite these mechanisms, significant oversight gaps persist in many countries, undermining accountability:

- **Lack of independent oversight bodies:** In some states, there is no independent authority focusing on surveillance oversight. Jordan has no dedicated data protection agency or privacy commission, and no requirement to report surveillance activities publicly. El Salvador's new 2024 data protection law pointedly failed to establish an independent data protection authority, instead concentrating enforcement powers under a new cybersecurity agency (ACE) that is tightly controlled by the President. This absence of independent eyes raises concerns that surveillance abuses will go unchecked. Pakistan, while drafting a Personal Data Protection Bill in 2023 that proposes a National Commission for Personal Data Protection, has not yet actually instituted such a body (the bill is still pending), leaving a current vacuum in civilian oversight of surveillance and data gathering.
- **Executive dominance and weakening of oversight:** Worrying trends include the dilution or abolition of oversight institutions. Mexico's 2025 legal reforms, for instance, abolished the constitutionally autonomous INAI, transferring its transparency and data protection duties to a government ministry and a new entity under executive influence. Critics argue this move "compromises independent oversight" over surveillance and information rights. In El Salvador, the new cybersecurity agency is termed "autonomous" but is in fact under presidential control, and its broad powers to demand data and sanction entities, without judicial or legislative checks, risk creating an unchecked surveillance czar in the executive branch. These developments point to a consolidation of surveillance authority in the executive at the expense of independent accountability.
- **Opacity and secrecy:** Even where oversight bodies exist, their effectiveness is often hampered by excessive secrecy invoked for national security. For example, Lebanon's Law 140 judicial commission operates behind closed doors with no public reporting. Jordan does not publicly disclose any spyware procurement or usage, and India's intelligence agencies traditionally function without any public reporting or parliamentary scrutiny (there is no parliamentary intelligence committee in India, and agencies are exempt from the Right to Information Act). In

Pakistan, the discovery of the LIMS system came not from proactive oversight but from an incidental court case, indicating that surveillance systems can be deployed without notifying even the courts or regulators, until a leak or legal challenge forces a spotlight on them. Meaningful accountability struggles against this wall of secrecy. As civil society observers frequently note, transparent oversight of surveillance is only as good as the disclosure requirements and enforcement powers behind it.

- **Enforcement and consequences for abuse:** A true test of oversight is whether misuse of surveillance is detected and punished. Here, too, the record is mixed:
 - In Serbia, recent court cases have started to hold authorities to account. A 2023 Administrative Court ruling decisively found that the security agency's spyware deployment "without proper judicial authorization" violated the right to privacy (Art. 8 ECHR), marking a rare instance of a domestic court in the region formally declaring a surveillance act unlawful. The outcome included a high court ordering a parliamentary inquiry into surveillance practices and recommending legislative reforms to align with EU standards. Likewise, Brazil's institutional response to spyware abuse has been robust. The Federal Police's "Operation Última Milha" investigated and raided intelligence officials who misused spyware to monitor journalists and even judges, and the federal audit court blocked government spyware acquisitions upon finding procurement irregularities. These actions show oversight bodies can ensure consequences, from suppressing illegally obtained evidence to triggering criminal investigations of officials.
 - On the other hand, in Jordan and Lebanon, there have effectively been no repercussions for confirmed spyware campaigns like Pegasus or the Dark Caracal operation. Despite evidence from Citizen Lab and Amnesty identifying dozens of Jordanian activists and journalists hacked by Pegasus between 2019-2021, no Jordanian court or prosecutor has taken up the issue, in a "profound accountability vacuum," as human rights groups put it. In Lebanon, the perpetrators of the Dark Caracal spyware ring (allegedly linked to a security agency) were never publicly investigated or sanctioned; no case was filed to address it. Even India, where the Pegasus scandal drew enormous attention, has seen limited accountability. The Supreme Court appointed an independent expert committee which confirmed malware on some journalists' phones but the government stonewalled on disclosures, and to date no officials have been held legally liable (the Court did insist that invoking "national security" does not grant a free pass from judicial review, an important principle, but practical follow-up has been slow). These examples underscore that oversight mechanisms are only effective if backed by the political will to act on findings. In more authoritarian climates, surveillance abuses often meet denial or impunity rather than accountability.

In summary, oversight of digital surveillance varies from relatively institutionalized systems in democratic states (with independent data regulators, judicial review, and transparency laws) to effectively unchecked surveillance in authoritarian contexts. Countries like Italy, Brazil, Kenya, Serbia, and (until recently) Mexico have built multi-faceted oversight architectures, combining independent regulators, judicial controls, and some legislative or public reporting, although even in these states oversight bodies struggle with resource and secrecy challenges. On the other hand, Pakistan, Jordan, El Salvador, and

Lebanon illustrate how surveillance can operate with minimal independent scrutiny, especially when national security is used as a blanket justification. One emerging pattern is the erosion or bolstering of oversight correlating with political trends. Where governance is becoming less accountable (e.g. El Salvador's power consolidation, Mexico's weakening of INAI, Jordan's crackdowns), oversight mechanisms are being curtailed; conversely, where the rule of law is holding (Brazil's post-authoritarian institutions, Kenya's constitutionalism, Serbia's EU aspirations), oversight, though imperfect, is gradually strengthening. Ultimately, the presence of independent, empowered oversight bodies and a culture of transparency significantly determine whether legal surveillance powers are kept within lawful bounds or become tools of unchecked repression.

4.4 Remedies and redress for individuals

Another critical aspect of a surveillance framework is whether individuals who are subjected to unlawful or excessive surveillance have any remedies or avenues for redress. Given the secret nature of surveillance, obtaining a remedy is challenging. Often, targets do not even know they were surveilled until after the fact - if ever. Still, the legal systems in these countries provide various (if limited) mechanisms for individuals to challenge surveillance or seek relief for violations of their rights:

- **Exclusion of illegally obtained evidence:** One practical remedy is in the context of criminal trials. If surveillance was conducted without due process, courts may suppress or exclude that evidence. This has been invoked in multiple jurisdictions. In India, high courts have suppressed interception orders that didn't meet legal safeguards and ordered that the intercepted communications be excluded from evidence, reinforcing that prosecutions cannot benefit from unconstitutional surveillance. For example, in *Vinit Kumar v. CBI* (2019), the Bombay High Court struck down three phone tap orders for lacking the required emergency grounds and recorded reasons, and deemed the recordings inadmissible. Similarly, in *Jatinder Pal Singh* (2022), the Delhi High Court held that using illegally intercepted calls would be "manifestly arbitrary" and violate fundamental rights, thus they could not be used in court. El Salvador's judiciary has also enforced technical compliance in criminal cases: trial courts have nullified wiretap evidence when prosecutors failed to obtain a timely judicial extension for surveillance beyond the 72-hour window allowed for adding new suspects, citing violation of the target's privacy and LEIT rules. These exclusions serve as a deterrent and a partial remedy. They protect defendants from convictions based on tainted surveillance and indirectly discipline law enforcement to follow procedure. However, exclusion of evidence only helps those who end up charged; if surveillance never leads to court proceedings (but is used for harassment or intelligence), this safeguard does not directly assist the victim.
- **Constitutional or human rights petitions:** Individuals (or public interest litigants) can file constitutional claims or *habeas corpus* petitions alleging that surveillance violated their fundamental rights. In some instances, courts have entertained such petitions even in the absence of a criminal case. For example, in Pakistan, as early as the 1990s, politicians like Benazir Bhutto brought constitutional cases against government eavesdropping. The Supreme Court in those cases condemned illegal surveillance as a breach of the right to life and dignity (Articles 14 and 9). More recently, when audio leaks and spying allegations surfaced, individuals approached the Islamabad High Court, which in 2024 took cognizance of the issue, leading to the exposure of the LIMS system and a ruling defending citizens' privacy against such mass surveillance. In Kenya,

litigants have filed constitutional petitions to stop intrusive tech deployments (e.g. the *Murage* case in 2015 sought to prevent a SIM technology rollout over interception fears), and while the courts didn't grant relief without concrete proof, they affirmed that one can petition the court if surveillance measures threaten constitutional privacy rights. Mexico's *amparo* (injunction) suits have also been used to challenge surveillance laws or practices. For instance, activists filed *amparos* against mandatory data retention and real-time tracking provisions, contributing to Supreme Court reviews that clarified limits on those powers. Thus, there is a pathway in many jurisdictions for individuals to directly invoke constitutional review of surveillance conduct, though it requires resources and, often, the public revelation of the surveillance.

- **Complaints to oversight bodies:** Where independent oversight agencies exist, individuals can lodge complaints there. Data protection authorities in Kenya and Serbia, for example, can receive complaints from citizens about misuse of their personal data, which could include unlawful surveillance or unwarranted data access. Kenya's ODPC, under its complaints procedure, can investigate and issue remedies such as ordering deletion of unlawfully collected data or imposing fines. In practice, such agencies are relatively new and have not yet dealt with high-profile national security surveillance complaints (which are often exempt or hard to investigate due to secrecy). Similarly, Kenya's Intelligence Service Complaints Board offers a formal channel for a person to report misconduct by intelligence officers. If, for example, a journalist suspects they were illegally surveilled, they could approach the board. The existence of these channels is important, but their effectiveness hinges on awareness and trust. Many affected individuals, especially in repressive contexts, may fear retaliation if they complain. It is notable that in more authoritarian settings (Jordan, El Salvador), no comparable independent complaint mechanism exists and victims of spyware or unlawful surveillance have no obvious domestic office to turn to.
- **Civil liability and damages:** Another form of redress is suing for damages or state liability. This is rare in the surveillance context, but not unheard of. A standout case is the Ziad Itani affair in Lebanon. Itani, an innocent playwright framed for espionage using fabricated digital evidence, later sued the state. In 2025, Lebanon's highest administrative court found the government liable for the harm he suffered, including the use of hacking to plant false evidence, and awarded compensation for violation of his rights. This is a rare instance of a court granting monetary redress tied to abusive surveillance practices - in this case, hacking and evidence fabrication. It signals that, at least in principle, individuals can seek reparations if they can prove the state's surveillance actions were unlawful and caused harm. However, such cases face high hurdles of proof and courage. In most countries, victims of secret surveillance might never have the proof or political climate to successfully sue the government for damages. Notably, no known damages cases have succeeded for Pegasus victims in these countries, though attempts have been made through international courts or complaints (e.g. journalists in El Salvador appealed to the Inter-American Commission on Human Rights, which urged a moratorium on spyware use).
- **International and regional remedies:** Where domestic remedies fail or are exhausted, individuals sometimes turn to international mechanisms. For example, surveillance-related complaints have been brought to the European Court of Human Rights (ECHR) by Serbian activists in the past (Serbia, though not an EU member, is party to the ECHR), and the 2023 Serbian Administrative Court ruling explicitly cited Article 8 of the ECHR (privacy right), laying the

groundwork for potential appeals to Strasbourg if needed. Greek journalist Thanasis Koukakis's lawyers [announced](#) in September 2026 that they had filed an application with the European Court of Human Rights (ECHR) against Greece over how the national judicial authorities had handled the investigation into the surveillance and spying on the reporter by the Greek National Intelligence Service. In the Americas, Salvadoran journalists took their Pegasus spying case to the Inter-American human rights system, seeking protective measures and pressure on the government. These international avenues can shine a spotlight and sometimes yield moral or political pressure, but they rarely provide direct relief to individuals in the short term.

In aggregate, the reality is that redress for surveillance abuses is limited. Legal frameworks may acknowledge a right to privacy, but enforcing that right *post hoc* is difficult when surveillance is covert. Affected individuals often learn of violations only through leaks or investigative reporting (e.g. the Pegasus Project revelations or Citizen Lab reports). Even then, pursuing remedies can be risky or fruitless if domestic institutions are unresponsive. The patterns that emerge are: in countries with stronger rule of law (e.g. India, Brazil, Mexico, Kenya, Serbia), we at least see courts willing to entertain challenges and sometimes provide remedies (exclusion of evidence, invalidation of unlawful laws, or even inquiries and damages in exceptional cases). In more closed environments (Jordan, current El Salvador, historically Pakistan's security sector), individuals have virtually no recourse, illegal surveillance tends to go unacknowledged by authorities, and raising a complaint may invite further harassment. Importantly, none of these countries have adopted a practice of notifying individuals that they were surveilled after the fact (a measure some suggest would enable legal challenges). Remedies therefore remain reactive and dependent on chance discovery. Strengthening redress requires greater transparency and whistleblower protections so that abuses come to light, combined with legal provisions explicitly allowing victims to seek relief. As it stands, the gap between formal rights and actual remedies remains wide, constituting a significant regulatory gap in the protection of journalists and citizens from unlawful digital spying.

4.5 General surveillance frameworks vs. spyware-specific rules

A pressing development in recent years has been the proliferation of spyware and state hacking tools (like NSO Group's Pegasus, FinFisher, or custom malware) which can deeply infiltrate devices. These tools often bypass traditional communication channels, raising the question: do existing surveillance laws cover their use, or are special rules emerging? Across the surveyed countries, most legal frameworks for surveillance were written with traditional wiretap and intercept techniques in mind, and few have been explicitly updated to regulate government hacking or spyware. This has created a regulatory gap that some states are just beginning to confront. Key observations include:

- **Few explicit spyware laws – notable exceptions:** Only a couple of countries have directly legislated on the use of spyware or hacking by authorities:
 - Italy is a pioneer among this group in formalizing rules for government hacking tools. In 2017-2019, Italy amended its laws to authorize the use of “*captatori informatici*” (computer trojans deployed by law enforcement) under strict conditions. Judicial warrants for such tools are limited to serious crimes (like terrorism or mafia cases), and the laws impose safeguards, such as strict judicial oversight on how the tool is deployed, filtering of irrelevant data collected, secure storage of extracted data, and adherence to

proportionality (mirroring European court guidance on surveillance). In essence, Italy extended its traditional intercept warrant framework to cover digital surveillance, treating it as an intrusive search that must be tightly controlled.

- El Salvador, conversely, took a problematic turn by effectively legalizing spyware use with minimal oversight. In 2022, amid a crackdown on gangs and dissent, El Salvador's legislature reformed its Computer Crimes Law to allow prosecutors to conduct "undercover digital operations" without prior judicial authorization, and created a category of "digital secret agents" empowered to access electronic communications. This vaguely-worded reform is widely interpreted as giving legal cover to government hacking or planting of spyware in investigations, all outside the normal warrant process. Human rights groups warned that this opened the door to Pegasus-style operations and even criminalized investigative journalism (since journalists could be swept up as targets or accused of "interference"). El Salvador stands out for explicitly authorizing spyware deployment but in a way that sidesteps independent oversight, essentially the opposite approach of Italy.
- **Most countries rely on general laws:** In the absence of dedicated spyware legislation, governments typically justify the use of spyware under existing legal provisions for interception or search:
 - In India, for example, there is no law that says "you may use spyware," but authorities argue that existing interception laws (the Telegraph Act, IT Act) and hacking prohibitions (IT Act Section 66) allow the government to hack devices if done with proper authorization, while it is illegal for any private actor. The Pegasus controversy revealed that such operations were happening with an unclear legal basis. The Supreme Court's intervention via an expert committee implicitly acknowledged spyware falls within the remit of surveillance needing oversight, as the Court rejected a "national security" carte blanche and examined whether any legal process was followed. However, India still lacks a statute that explicitly governs government malware use; it remains a grey area addressed via general privacy and hacking laws.
 - Pakistan similarly does not mention spyware in law, but its agencies reportedly acquired tools like FinFisher in the 2010s. The exposure of the LIMS mass interception system (an automated tapping tool) highlights that new surveillance technology was deployed without a dedicated legal framework, and only came to light through court proceedings. Any legal review of spyware use would likely fall under general privacy and cybercrime laws (PECA 2016 criminalizes unauthorized access to devices, so state use would have to be shoehorned into some "authorized" category, perhaps under broad warrants or emergency powers). Currently, Pakistan has no explicit rules detailing if or how agencies can hack devices, an omission common to many states.
 - Kenya, Brazil, Mexico, Serbia and Lebanon all have robust intercept laws and privacy statutes, but none explicitly spell out rules for deploying spyware against a target. In theory, any hacking of a device to intercept communications should require the same sort of warrant as a wiretap or a computer search. For instance, Kenya's CMCA (2018)

authorizes judges to issue warrants for “real-time collection of traffic data” and “interception of content”, which could be interpreted to cover techniques like keylogging or Trojan installation as means of interception, as long as a warrant is obtained. Serbia’s laws would similarly treat device hacking as a form of surveillance that requires a court order under the Criminal Procedure Code, and if done without one, it is a crime (the cases of police using Cellebrite and NoviSpy in 2023 were deemed unlawful for lack of prior court approval). Mexico’s framework requires a federal judge’s warrant for any form of interception or tracking (content or metadata), so even Pegasus use should legally be subject to a warrant. The scandal in Mexico was that Pegasus was apparently used without proper judicial authorization on journalists and activists, implying a violation of existing law. The Mexican Supreme Court hasn’t directly ruled on spyware’s legality, but it has strongly underscored that all surveillance measures, including new technologies, must stay within constitutional bounds of authorization and purpose.

- Lebanon’s law 140/1999 was forward-looking for its time but didn’t anticipate modern spyware. It covers telephony and “wireless communications” broadly, so arguably hacking a phone to eavesdrop is an “interception” requiring a warrant or ministerial order. The Dark Caracal operation, which involved tricking targets into installing malware via fake apps, took place outside any legal process, constituting an intelligence operation with no judicial sign-off. Lebanese law enforcement and courts have so far not addressed whether evidence obtained via spyware (without following Law 140) would be admissible or not, leaving a void. Civil society notes that no-one was held accountable or even tried for deploying spyware in Lebanon. This is representative of many countries, where the legal framework does not explicitly permit it, but also does not explicitly punish state actors for using it, thus creating a loophole of deniability.
- **Judicial scrutiny and emerging norms:** In absence of clear legislation, courts and other institutions are starting to articulate norms around spyware:
 - Brazil’s judiciary is taking a proactive stance. The Prosecutor-General’s Office filed a petition (*ADPF 1143*) in late 2023 to suspend all use of spyware by public authorities until a legal framework is in place, arguing that current use lacks a legal basis and oversight. The Supreme Federal Court responded by holding unprecedented public hearings in 2024 on spyware, gathering input from experts and civil society. This indicates an emerging consensus that digital intrusion tools demand special safeguards. Additionally, Brazilian authorities like the Federal Audit Court (TCU) stepping in to halt spyware procurement (Harpia system in 2021) show recognition that unchecked spyware deployment is dangerous and needs at least ex ante review or rules. We see Brazil attempting to fill the gap through judicial and quasi-judicial means pending legislation.
 - Mexico’s courts, as noted, enforced transparency around Pegasus, which, while not regulating its use, at least brings some accountability. By ordering agencies to release information on spyware contracts and not allowing them to hide behind secrecy entirely, the courts are indirectly saying spyware is not above the law. This sets the stage for

potential future litigation if evidence arises of misuse. Armed with information, victims could challenge the government on constitutional grounds.

- Courts elsewhere have scarcely touched the issue. In Jordan, not a single case on Pegasus or similar has been filed, illustrating judicial inaction (or intimidation) on this topic. In Serbia, a few cases have begun tackling the use of device extraction tools and covert apps, with mixed results - one court excused it citing national security, another condemned it as illegal. This divergence shows the norm is still evolving domestically. Lebanon's judiciary has indirectly engaged via the Itani case (punishing fabricated digital evidence), but it framed it more as a torture/abuse issue than a privacy violation, thus sidestepping a direct pronouncement on spyware's legality.

In summary, most countries still regulate digital surveillance primarily through general frameworks (wiretap laws, computer misuse laws, privacy statutes) that did not specifically contemplate modern spyware. The risk is that government hacking tools slip through the cracks of these laws. Agencies may argue that deploying spyware is not "interception" in the classic sense or may operate in secret with no one the wiser to challenge them. The exceptions are revealing: Italy shows that it is possible to explicitly bring spyware under the rule of law (but only a few advanced democracies have done so thus far), whereas El Salvador shows how spyware can be given a legal framing in a way that diminishes oversight (essentially legislating around judicial control). The lack of spyware-specific safeguards is a persistent gap in national laws. However, growing public scandals have put pressure on governments and courts. A pattern of convergence might be emerging, since international human rights bodies (UN experts, IACHR, etc.) are calling for moratoria or strict conditions on spyware, and some national courts (Brazil, India to a degree, Mexico) are responding. Until dedicated legislation catches up – for example, a law requiring that any use of malware to surveil must have a time-bound warrant, minimization protocols, and oversight reporting – the treatment of spyware remains patchy. For now, it largely falls to judges and oversight agencies to read spyware into existing rules (ensuring it is treated as any other intercept/search requiring authorization) and to expose abuses when they occur. This is clearly an area in flux, representing a significant regulatory frontier in the fight to protect journalists and citizens from the most invasive surveillance technologies.

4.6 Regional and systemic patterns

Across the ten countries, certain regional and systemic patterns become evident, revealing how political context, level of democratic governance, and international frameworks influence surveillance regulation. While each country's framework has unique nuances, we can identify trends that differentiate democratic vs. authoritarian-leaning practices, as well as some common gaps that transcend geography:

- **Influence of democratic governance and rule of law:** Broadly speaking, countries with stronger democratic institutions and rule of law tend to have more robust formal safeguards and somewhat more accountability in practice. Italy, the only EU nation among the case studies, exemplifies a Western European standard. Its laws are tightly aligned with European human rights norms, requiring judicial warrants and proportionality, and it benefits from supra-national oversight like the European Court of Human Rights and EU Court of Justice rulings that strike down disproportionate measures. For example, Italy had to adjust its data retention practices after EU rulings against blanket retention. Italy's incorporation of GDPR and the Law

Enforcement Directive has modernized privacy oversight for both private and police data processing, and its moratorium on facial recognition shows a precautionary, rights-driven approach. The European context clearly elevates privacy as a core value, forcing strict legal discipline for surveillance. Similarly, countries aspiring to or influenced by European standards, like Serbia, have on paper adopted EU-style data protection laws and judicial warrant requirements. Serbia's laws look very strong on paper (thanks to EU alignment); however, in practice the gap between law and enforcement can be wide. Observers note that while Serbia formally meets European benchmarks, political pressures and weak institutions mean surveillance abuses (especially by intelligence agencies) still occur with limited transparency and enforcement. Media [reports](#) in September 2026 exposed the largest documented wave of surveillance in Serbia, including the use of the Pegasus spyware. This underscores that democratization of law does not automatically translate to democratization of practice; political will and independent oversight are needed to bridge the gap.

- **Global South democracies and legal reform:** Several Global South democracies in this list (India, Brazil, Mexico, Kenya) have undertaken significant legal reforms, often inspired by international norms, to strengthen privacy and regulate surveillance. For instance, Brazil, Mexico, and Kenya have all enacted comprehensive data protection laws in the last decade (LGPD 2018 in Brazil, Kenya DPA 2019, Mexico's new 2025 data laws) which embed principles of consent, purpose limitation, and oversight. These often mirror the EU's GDPR, reflecting a global convergence on privacy standards. Each has also affirmed the necessity of judicial warrants for interception in their constitutions or apex court rulings, demonstrating a common commitment to due process across very different regions. Additionally, their judiciaries have been active. Brazil's Supreme Court has been a bulwark against excessive surveillance (protecting WhatsApp encryption, requiring judicial control for financial data access, etc.); Mexico's Supreme Court has struck down laws that overreached (biometric SIM registry, warrantless military intercepts). Kenya's courts are carving out a role by demanding data protection impact assessments and public participation before rolling out surveillance tech, something quite unique in the African context, signalling a judicial willingness to enforce constitutional privacy. These trends show that many Global South democracies are actively trying to balance security and privacy, often under the influence of global human rights discourse and sometimes learning from each other's experiences. For example, Kenya's ODPC and Nigeria's upcoming DPA were influenced by Ghana's and the EU's models. Brazil's LGPD was inspired by Europe but adapted to local context. There is a kind of South-South and North-South dialogue visible in these reforms.
- **Authoritarian contexts and surveillance as control:** In more authoritarian or hybrid regimes, such as Pakistan, Jordan, El Salvador (under Bukele), and to an extent Lebanon, the pattern is that while some formal laws recognize privacy or impose warrants, in practice the security sector wields surveillance as a tool of political control with fewer checks. Jordan is a clear example. Despite documented Pegasus abuses against activists, the legal system offers no meaningful check or remedy, and new laws (like the 2023 cybercrime law) are instead empowering authorities to police online speech and seize devices without warrant. The emphasis is on controlling dissent rather than regulating surveillance powers, and surveillance operations remain shrouded in state secrecy with virtually no independent oversight. El Salvador's trajectory in the last few years shows a rapid erosion of checks in the name of security, and

although constitutional guarantees exist, they have been effectively suspended or circumvented through emergency decrees and legal reforms that centralize surveillance in the executive. This has enabled systematic spying on journalists and civil society (as uncovered through Pegasus forensics) with impunity. Pakistan lies somewhere in between. It has democratic practices and courts that sometimes speak up (the IHC's expose of the LIMS system was a bold move), but the powerful military and intelligence establishment often operate above the law. The Supreme Court's quick stay of the IHC's attempts to restrain LIMS hints at institutional deference to the security apparatus. Pakistan's approach to surveillance is heavily driven by internal security priorities (counter-terrorism, monitoring political opposition), and while privacy is a constitutional right, enforcement is inconsistent. Lebanon presents a nuanced case: not exactly authoritarian, but a relatively weak state with strong security agencies. It has a detailed surveillance law, yet the government itself violated it for years with large-scale data grabs, and accountability was minimal. This suggests that in environments with high security threats or political instability, surveillance oversight erodes, either by deliberate policy (as in Jordan, El Salvador) or due to institutional weakness (Lebanon, Pakistan).

- **Global norms and pressure:** International norms and pressure play a role in shaping surveillance laws, especially in countries that seek global integration or aid. EU influence is notable. Italy and Serbia align with EU privacy and human rights standards; Kenya's and Brazil's adoption of GDPR-like laws also reflect an international normative pull (and desire to facilitate data flows with Europe). Inter-American human rights standards have had an impact in Latin America. The IACHR has been vocal about surveillance threats to journalists (e.g., calling out El Salvador and urging safeguards), and Latin American courts seem receptive to these human rights arguments. In Asia and the Middle East, the influence is less uniform, though UN special rapporteurs have repeatedly highlighted issues like spyware and the need for moratoria, which provide civil society and courts with persuasive authority to demand change. For instance, the UN Cybercrime Convention negotiations and other UN resolutions have spurred debates in countries like India and Brazil on the acceptable scope of lawful surveillance. It is possible to observe some convergence in rhetoric, since virtually all these governments publicly acknowledge that surveillance must be lawful, necessary, proportionate, etc., showing the success of human rights discourse. The divergence is in implementation.
- **Persistent gaps across regimes:** Regardless of North/South or democratic/authoritarian divides, some regulatory gaps are common:
 - *Spyware and advanced technology:* Few countries have fully caught up with regulating state malware and other modern surveillance tech. This gap is present in liberal democracies and authoritarian states alike, although democracies are beginning to respond (through courts or updated laws), while authoritarian regimes exploit the gap maximally.
 - *Oversight of intelligence agencies:* Intelligence and national security operations are often shielded from transparency everywhere. Even in Italy, historically, services operated with a lot of secrecy (though under parliamentary committee oversight). In India, intelligence agencies have no statutory charter and are not directly accountable to Parliament or any external watchdog. Serbia had to strike down parts of its Intelligence Agency law for

being too vague, indicating how often these agencies push for broad leeway. Practically every country struggles with ensuring that intelligence bodies are kept within legal bounds.

- *Remedies for victims:* The lack of notification to surveillance targets and barriers to litigation mean that individuals whose rights are violated rarely see justice. This is a global problem; it is structural since secrecy is inherent to surveillance. Only a handful of cases (Itani in Lebanon, Ristić in Serbia, Pegasus FOI in Mexico) have yielded direct relief or recognition for victims, which is little comfort given the scale of the issue.

Ultimately, the comparative picture shows converging recognition of principles, but diverging implementation. All these countries recognize privacy and due process in theory, and most have updated or are updating their laws to address digital surveillance. However, the effectiveness of those protections tracks the broader governance context; liberal democracies and countries with active civil societies are progressively refining their surveillance oversight (though even they struggle with new tech), whereas authoritarian or hybrid regimes are either standing still or backsliding, using new technologies to reinforce state power in spite of legal niceties. A persistent theme is the need for stronger independent oversight and clearer rules on emerging surveillance methods, gaps that exist even in advanced systems but are glaring in others. Without these, even the best-written laws can be overridden by executive fiat or quiet technical intrusions. The analysis therefore points to an overarching conclusion that legal frameworks are only as good as the institutions that enforce them, and bridging the gap between law and practice remains the key challenge globally in protecting journalists and citizens from undue digital surveillance.