

A PRIVACY NIGHTMARE:

UNDERSTANDING SPYWARE



Edited by
Andrej Petrovski & Danilo Krivokapić

A PRIVACY NIGHTMARE:

**UNDERSTANDING
SPYWARE**

Impresum:

Editors:

Danilo Krivokapić & Andrej Petrovski

Authors:

Bojan Perkov, Filip Milošević & David Stevanović (Technology)

Tijana Stevanović (Legal)

Andrijana Ristić & Mila Bajić (Practice)

Design and art direction:

Olivia Solis Villaverde, Vladan Joler

Language editing:

Milica Jovanović

SHARE Foundation, 2025

ACKNOWLEDGEMENTS

We would like to thank our colleagues from the SHARE Foundation for all the support and contributions in the process of writing this book, as well as all their work in analysing and documenting the illicit use of spyware in Serbia.

We would also like to thank all partners who have contributed to this book and to building our capacities to understand the complexities of spyware: Access Now, Amnesty International, EDRi, The Citizen Lab, PEGA Coalition and the Spyware Accountability Initiative.

Special thanks to all the experts who contributed to the Legal part by sharing information from their countries: Aljoša Ajdanović Andelić (Spain), Amber Sinha (India), Ana Gaitán Uribe (Mexico), Anella Buković (Croatia), Asli Telli (Turkey), Duje Kozomara (Croatia), Duje Prkut (Croatia), Eleftherios Chelioudakis (Greece), Laura Nathalie Hernández Rivera (Guatemala), Olga Cronin (Ireland), Simone Ruf (Germany), Siti R. A. Desyana (Indonesia) and Wojciech Klicki (Poland)

We dedicate this book to the people of Serbia who fight for a just and free society and especially to the students and professors who are at the forefront of that fight. Your courage and energy are the main inspiration for our work.

Thank you,

The Authors

“Nothing was your own except the few cubic centimetres inside your skull.”

— George Orwell, 1984

INTRODUCTION

The appetite for power and control has driven the development of surveillance technology to a level that could only be found in the works of science fiction. A lot of the concepts designed during the Cold War have, since its end, been repurposed by governments to keep tabs even on allies, and eventually their own citizens. This techno-military-industrial complex has pierced through any ethical and human rights safeguards, aiming to kill privacy and create a market now worth hundreds of billions globally.

While corporations that produce surveillance technology thrive in times of crisis, such as pandemics, wars and political instability, governments that feel threatened by legitimate political unrest in their countries perceive surveillance as the low-hanging fruit that might help them cling to power longer.

In our previous book, *Beyond the Face: Biometrics and Society*, we tried to understand in what state the world was vis a vis the usage of biometric surveillance after the COVID-19 pandemic and just before the EU AI Act was negotiated and adopted. The research process behind it lasted for almost five years, at which point our understanding of biometric surveillance had reached a fairly profound level.

This time, the task was more difficult. Spyware is a far more complex concept. In essence, governments and corporations are (often working together) developing malware to infect the smartphones of individuals of interest. The pretext is, of course, battling crime and national security, despite the fact that there is no evidence of the effectiveness of this technology in such scenarios. Both the development and the use of spyware are highly secretive and opaque. We therefore had to rely on the limited public information available after cases of abuse were discovered, and on the skills of our colleagues and partners who perform forensic analysis on infected devices.

It was equally complex to analyse the legal framework across multiple jurisdictions, as there is no global standard for regulating the use of spyware. To be clear, we do not advocate for a specific regulation of the use of spyware for two main reasons: the first being that we consider it illegal under existing legislation regulating the production and use of malware; and the second

because a spyware-specific regulation, unless it is a total and absolute ban, will open the door for broad exceptions, which will practically legalise its use.

Although over the last two years we have documented grave misuse of spyware in Serbia, impacting the lives of many activists, journalists and other human rights defenders, including our team, we tried to go beyond our own context and look at other parts of the world, eventually confirming its detrimental effect on human rights, regardless of geography.

We hope that this book will be a useful tool to everyone who is working on protecting the right to privacy in these difficult times. Finally, we hope that it will reach decision-makers and help them understand that by allowing companies to produce spyware and governments to spy on their own citizens, as well as across borders, we might be the generation that killed privacy.

Danilo Krivokapić and Andrej Petrovski

CONTENTS

06 INTRODUCTION

11 TECHNOLOGY

- 13 SPYWARE IS MALWARE
- 27 THE “NEED” FOR SPYWARE
- 37 INFECTION PROCESS
- 49 COMMUNITY AND INDUSTRY RESPONSES

55 LEGAL

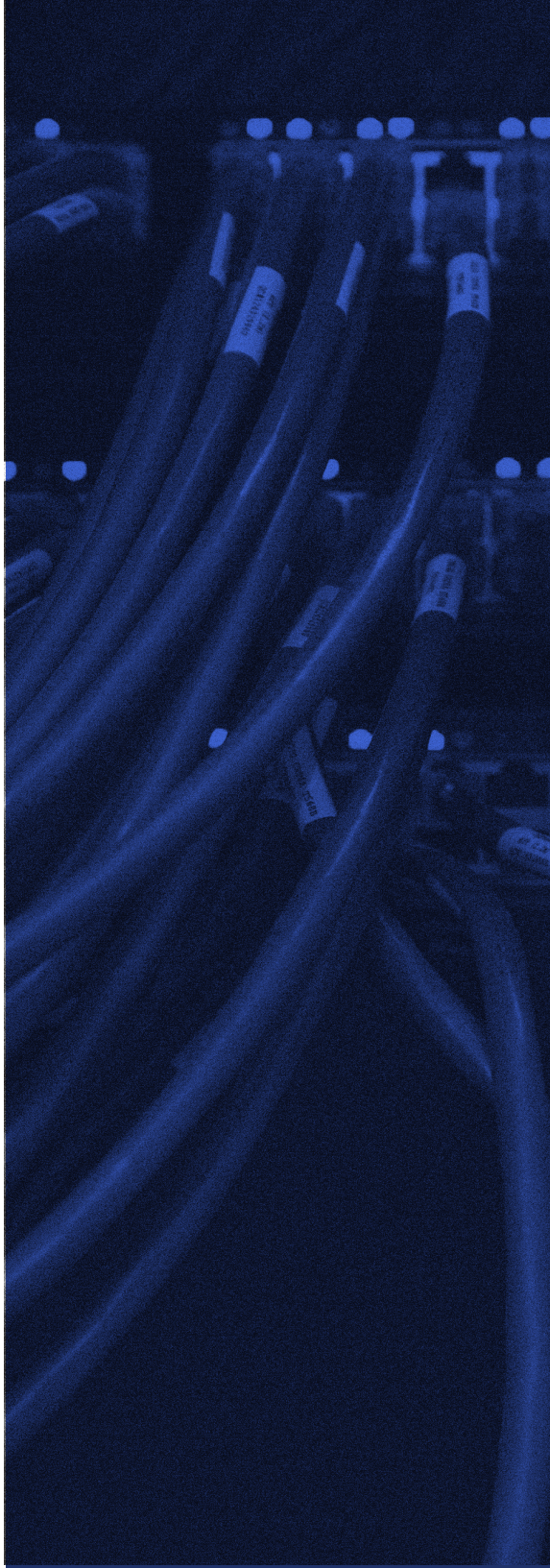
- 60 CROATIA
- 66 GERMANY
- 72 GREECE
- 78 GUATEMALA
- 82 INDIA
- 88 INDONESIA
- 94 IRELAND
- 100 ISRAEL
- 104 MEXICO
- 110 POLAND
- 114 SERBIA
- 118 SPAIN
- 124 TURKEY

133 PRACTICE

- 133 INTRODUCTION
- 145 SPYWARE AS A SYSTEMIC THREAT TO HUMAN RIGHTS
- 177 SPYWARE INC
- 189 SPYWARE ON DEMAND: NEW TOOLS, OLD BEHAVIOURS

278 ENDNOTES

A PRIVACY NIGHTMARE: UNDERSTANDING SPYWARE





TECHNOLOGY

TECHNOLOGY

Spyware has evolved from crude keyloggers and adware in the 1990s into today's highly sophisticated surveillance systems capable of silently compromising phones and computers. This section follows that trajectory: it begins by defining spyware and situating it among other forms of malware, before tracing its origins and rise alongside the spread of smartphones. It then turns to the commercial and state ecosystems that drive its development, and the technical toolkits – zero-day exploits, spyware agents, and command-and-control servers – that make these operations possible. With examples such as Pegasus, Predator, and NoviSpy, the discussion shows how spyware outpaced traditional wiretapping, exploiting device vulnerabilities to bypass encryption. From there, the focus shifts to how infections actually occur – through one-click links, zero-click exploits, network injections, or physical access – and to the risks these tools pose for human rights and digital security. The section closes with the ways researchers, civil society, and industry actors are working to detect and counter spyware, even as defenses remain fragile.

SPYWARE IS MALWARE

As digital technologies have become increasingly central to our globalized society, threat actors have sought to disrupt computers or compromise the information they process. Because information systems now play a crucial role in governing our lives and societies, they have also become prime targets for malicious activity. With more and more everyday devices connected to the internet – even household appliances like refrigerators and washing machines – the problem of malicious targeting is unlikely to disappear. The promise of the “Internet of Things” may well turn into the “Internet of Insecure Things”. Or, as cybersecurity expert Mikko Hypponen puts it, “if it's smart, it's vulnerable”.¹

One of the most common ways to disrupt the normal operation of software or hardware is by infecting it with malware. Merriam-Webster broadly defines malware as “software designed to interfere with a computer's normal functioning”,² while the US NIST Computer Security Resource Center glossary describes it as “software or firmware intended to perform an

unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system”.³ Confidentiality, integrity, and availability⁴ are the core security components of any information system – if any one of them is compromised, the data processed by the system is also considered compromised.

Malware comes in many shapes and forms, each of which has evolved over the past several decades. Trojans, for example, disguise themselves as safe or reliable software but, once downloaded, can take control of information systems for malicious purposes. Worms exploit vulnerabilities in operating systems to gain access to networks, which can then be used to launch DDoS attacks, steal sensitive data, or initiate ransomware campaigns.⁵ Depending on the motive – whether monetary, political, or military – malware can be directed against a wide range of targets: financial institutions, critical infrastructure such as power grids or water supply systems, or even an unsuspecting individual who happens to click on a fraudulent link. Without proper safeguards, incident response, and disaster recovery plans, large-scale malware attacks can inflict immense, sometimes irreparable, damage on critical information systems.

DEFINING SPYWARE

A specific type of malware – and the focus of this study – is spyware. The NIST Computer Security Resource Center defines it broadly as “software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code”.⁶

Unlike other types of malicious applications, spyware is not primarily designed to disrupt the operation of a device or network, nor simply to gain silent access for later attacks. Its main purpose is to extract information stored and processed on the targeted device. In this sense, while the immediate target of spyware is the device itself, the true objective – and the more valuable prize – is the information and personal data it contains.

As European Digital Rights (EDRi) – a coalition of more than 50 organizations at the forefront of protecting digital rights in Europe and beyond – explains in its position paper on spyware, the absence of a precise and enforceable definition has made regulation difficult. EDRi advocates

for a “full EU-wide ban on the development, production, marketing, sale, export, and use of spyware, grounded in a clear and enforceable definition that captures its core characteristics and functionalities”.⁷ The key issue, EDRi argues, is to define spyware by what it does – not by who uses it or how it is marketed – so that the definition remains enforceable and resilient. The definition should also be broad in scope, ensuring that future software with the same capabilities cannot be excluded, which would otherwise create loopholes and opportunities for abuse.⁸

According to EDRi, software should be defined as spyware if it meets the following elements:

- » Installed or run on a device **without the free and informed consent** of the user (the target).
- » **Compromises the integrity of the device.**
- » Delivered primarily by exploiting **existing or manufactured vulnerabilities** – including social engineering, physical implantation, pre-installed mechanisms, or deceptive ads.
- » **Operates remotely** after installation, meaning there is no need for physical access to the device once it has been infected.
- » **Targets specific individuals or groups**, or can be deployed **indiscriminately**.⁹

Taken together, these criteria show how broad the scope of spyware can be. To illustrate what falls within such a definition, the following categories are commonly recognized:

- » **Commercial spyware** – Privately developed with advanced capabilities, such as NSO Groups’ Pegasus or Predator, a product of the Intellexa Group.
- » **State-developed spyware** – For example, Germany’s *Remote Communication Interception Software* (RCIS) and Serbia’s Android spyware “NoviSpy” identified by Amnesty International’s Security Lab as likely state-made.
- » **Stalkerware** – Applications used by private individuals to surveil and abuse others, often in intimate relationships. Frequently

linked to domestic violence, these tools are sometimes disguised as “parental control” software.

- » **Parental control or employee monitoring software (bossware)** – Not all such tools are spyware, but those that allow remote, covert, and non-consensual access to communications or device settings fall under this category.
- » **Keyloggers** – Spyware that covertly records keystrokes, granting access to passwords, correspondence, financial information, and more.
- » **Infostealers** – Designed to extract user data such as browsing history, credentials, cookies, and files from infected devices.¹⁰

Although spyware – especially advanced or so-called “military-grade” modules – is a powerful surveillance tool, it is not the only technology used for targeted monitoring. Other tools can also access and exfiltrate a target’s communications, movements, contacts, and social circles. For example, Cellebrite UFED, a device used to unlock encrypted or password-protected phones and extract data for forensic or investigative purposes, has been repeatedly misused to access journalists’ phones.¹¹ Such tools are best described as spyware-enabling technologies – not spyware per se.

Not all surveillance tools fall under the definition of spyware. Remote desktop software such as TeamViewer or AnyDesk, for example, requires user consent that can be revoked at any time. Similarly, the collection of low-sensitivity telemetry data – such as error reports or usage statistics – by software vendors is not considered spyware. Traditional methods of surveillance carried out in accordance with the law, including court-approved wiretapping, lawful interception, or access to telecommunications metadata, also fall outside this category.¹² Beyond these, a wide range of tools and devices – from analytics software like Maltego¹³ or Griffeye¹⁴ to hardware such as IMSI catchers – can serve surveillance purposes but are not classified as spyware.

MALICIOUS ORIGINS

Spyware first appeared in online discussions in the 1990s, but it was only in the 2000s that it became a significant topic within the cybersecurity

industry. All varieties of spyware are designed to gather information, but the more advanced forms go further – modifying infected systems and exposing them to additional risks and cyber threats.¹⁵

The mid-1990s saw the emergence of keyloggers – simple programs designed to capture information such as typed passwords or chat logs. These were spread through floppy disks or by tricking unsuspecting users into downloads, at a time when most people online were unfamiliar with such privacy risks. As internet use grew rapidly between 2000 and 2004, some free software (freeware) began to include advertising modules that tracked user activity. This “adware” could be classified as spyware, though its main function was to flood users with advertisements, pop-up windows, or redirects to affiliate websites. Spyware, by contrast, operates stealthily and aims to remain hidden on the infected system. Adware created a lucrative revenue stream through online advertising, but over time its modules became more advanced, infiltrating deeper into users’ systems and moving closer to typical spyware. By the late 2000s and early 2010s, the corporate sector became a primary target for digital espionage – sometimes through seemingly “legal” tracking and surveillance tools, though trojan-based espionage soon became more prominent.¹⁶

With smartphones becoming mainstream in the 2010s, spyware expanded to target not only mobile operating systems such as Android and iOS, but also PCs and servers – evolving into cross-platform threats. Mobile spyware, often disguised as malicious apps, could secretly record calls and GPS data.¹⁷ Because smartphones now store vast amounts of professional, personal, and potentially compromising information, it was inevitable that they would become prime targets for intelligence and security agencies, the military, police, and other state actors. Espionage on behalf of powerful private or corporate interests has also become easier, since a mobile device is something a person carries with them almost constantly. When spyware is combined with other techniques – such as open-source intelligence (OSINT) searches or the purchase of personal data like email addresses and phone numbers from data brokers – defending against modern surveillance efforts becomes extremely difficult.

As spyware has entered private relationships, stalkerware and employee monitoring software (often called bossware) have further exacerbated unlawful surveillance and harassment. These tools typically require highly intrusive permissions on a device – such as the ability to activate

the camera and microphone, access photos and video recordings, create in-app screenshots, track location, or monitor the use of specific apps and features. Newer versions of iOS and Android prompt users to confirm such permissions, for example when recording a video. But if the device is physically taken from the target, the permissions can be enabled without their knowledge or consent – or the targeted individual may be manipulated into granting them under the guise of necessity or for their “own good”. Installation can happen either through coercion or without the user’s knowledge, since physical access to the device is often enough. In workplace settings, company-issued laptops or phones may also come with pre-installed surveillance apps that employees cannot remove or disable because they lack the necessary administrative privileges.

Needless to say, these apps are not only highly intrusive to a person’s privacy – they also expose users to a wide range of digital security risks. For example, a data leak from the employee tracking software WorkComposer, which logs keystrokes and captures screenshots, revealed more than 21 million images of employee activity.¹⁸ These screenshots could contain sensitive information such as salary details, health data, private correspondence, or online searches. Survivors of partner abuse may also face further harassment and exposure of their private lives when such data is leaked. The final part of this publication will examine these social dimensions of stalkerware and bossware in greater detail.

SPYMASTERS FOR HIRE

With the rapid expansion of both software and hardware, surveillance tools such as spyware have continued to evolve and adapt to new contexts. The commercial spyware market has grown to unprecedented levels, especially over the past decade, with products becoming increasingly sophisticated. Private vendors now play a central role in enabling state actors to target political opponents, human rights activists, and investigative journalists – a demand that fuels the development of ever more intrusive tools. As Amnesty International explains, “the surveillance industry develops spyware to bypass the increasingly strong security defenses in computer, mobile devices and communication platforms. Surveillance operators want to compromise devices so they can access all the data stored there.”¹⁹

The lack of technical expertise among many state actors to develop advanced spyware in-house, combined with weak regulation of the espionage market and rising authoritarian tendencies worldwide, has fueled demand for highly intrusive technologies. In this environment, the private spyware industry flourishes – effectively offering “despotism-as-a-service”, as Citizen Lab puts it.²⁰ Some states have managed to build and deploy their own spyware, such as the RCIS developed by Germany’s Federal Criminal Police Office (BKA).²¹ Israel, however, stands out: its cyber warfare Unit 8200 has become a pipeline feeding the country’s booming IT sector, particularly its spyware vendors, several of which are now known for producing highly sophisticated surveillance tools.²²

Spymasters’ toolkit

What sets modern advanced spyware apart from earlier products is its technical complexity and its deliberate focus on exploiting vulnerabilities – the entry points into the most sensitive parts of software and hardware. Once a vulnerability is successfully exploited, the targeted system may behave unpredictably, giving the attacker full control of the device and access to functions and privileges that would normally be off-limits. These vulnerabilities are both rare and difficult to exploit, but advanced spyware vendors employ top-tier talent capable of identifying weaknesses, developing exploits, and carrying out attacks – often without the knowledge of the manufacturer or the target.

Zero-day vulnerabilities – weaknesses in hardware or software that are unknown to the manufacturer or vendor – can remain “in the wild” for weeks, months, or even years before they are discovered and patched.²³ At the same time, ordinary users cannot be expected to maintain flawless digital hygiene. Outdated or unsupported operating systems, insecure applications, and limited digital literacy create a perfect storm that benefits threat actors of all kinds, from low-level cybercriminals seeking quick profit to state-sponsored hacker groups with advanced capabilities.

Vulnerabilities are exploited through malicious code known as exploits – programs designed to take advantage of security flaws in hardware or software and deliver the main piece of malware.²⁴ In simple terms, exploits function like lockpicks, allowing attackers to tamper with a system’s defenses and gain unauthorized control. Over the years, security researchers have uncovered many sophisticated spyware exploits “in the wild”. One notable example is FORCEDENTRY, an exploit for Apple’s iMessage uncovered by Citizen Lab in 2021. FORCEDENTRY was both a zero-click and a zero-day exploit used to deploy Pegasus spyware – meaning it required no action from the targeted individual (no need to click a link), and Apple was unaware of the vulnerability until it was reported. The exploit targeted Apple’s image rendering library by sending a malicious payload made up of 27 identical files disguised as .gif images. This trick enabled arbitrary code execution, allowing attackers to run their own malicious code on the device.²⁵

The main product – the spyware agent itself – is deployed once a vulnerability has been successfully exploited. Amnesty International defines a spyware agent (or “implant”) as the final piece of code installed on a device after infection. The agent collects data, activates sensors such as microphones and cameras, and sends this information back to the operator.²⁶ Depending on the customer’s needs and the target’s profile, spyware agents can be tailored to attack different devices, operating systems, and applications. Once “inside”, advanced spyware agents are extremely difficult to detect without a forensic examination of the device and its data. They often disguise themselves as harmless system apps or processes and are designed to erase digital traces of their presence, making it increasingly challenging for investigators to confirm an infection.

What sets commercial spyware vendors apart from other invasive tech companies is that they offer a full range of espionage services to their customers. Many sell so-called “end-to-end” spyware systems – complete toolkits for device infection and data collection. These systems include the exploits used to install the spyware, the spyware agent that runs on the infected device, and the back-end infrastructure for gathering and analyzing stolen data.²⁷ Vendors do not stop at developing exploits and agents: they also maintain a complex ecosystem of domain names, phone numbers, email accounts, and servers. These servers, often referred to as command-and-control (C2) servers, form the “back end” of spyware operations, issuing commands to infected devices and retrieving information from

them. Investigative organizations rely on infrastructure analysis tools such as Shodan²⁸ and Censys²⁹ to expose these espionage assets and link them to spyware vendors. But vendors, in turn, go to great lengths to hide their tracks – frequently abandoning or “burning” infrastructure once it has been discovered and made public.

Advanced capabilities uncovered

Some of the first spyware tools with advanced capabilities to draw sustained public attention were Hacking Team’s Remote Control System (RCS) and FinFisher/FinSpy. From the early to mid-2010s, investigative reports and forensic analyses began documenting their deployment, revealing not only widespread use but also technical details about how these products operated. This marked a turning point in the public awareness of commercial spyware: it was no longer a hidden niche but a recognizable and debated threat in the broader cybersecurity and human rights communities.

In 2014, the Citizen Lab made public a series of investigations into hacking attempts against Ethiopian journalists. These attacks involved the deployment of Hacking Team’s Remote Control System (RCS), a trojan capable of extracting a wide range of files and communications from targeted devices. RCS could copy documents from a hard drive, record Skype conversations, activate a computer’s camera and microphone, and capture both email and instant messaging chats. Its main selling point was the ability to intercept information before it was encrypted—precisely the kind of access government agencies seek when expanding their surveillance capabilities.

The Ethiopian journalists were targeted with malicious executable files (.exe), disguised as articles in PDF or Microsoft Word (.doc) format, and delivered via Skype communications. Citizen Lab’s analysis revealed that these files connected to a server under Hacking Team’s control.³⁰ Beyond desktop targets, Hacking Team also distributed a corrupted version of an Android news app focused on Saudi Arabia. Once installed, this implant demanded intrusive permissions, including access to calls, SMS messages, and location data. Even more troubling, it could escalate to root privileges, enabling deep manipulation of the device, such as altering file permissions.³¹

FinFisher, marketed by Gamma International as a government-grade intrusion and remote monitoring solution, became notorious for its role in

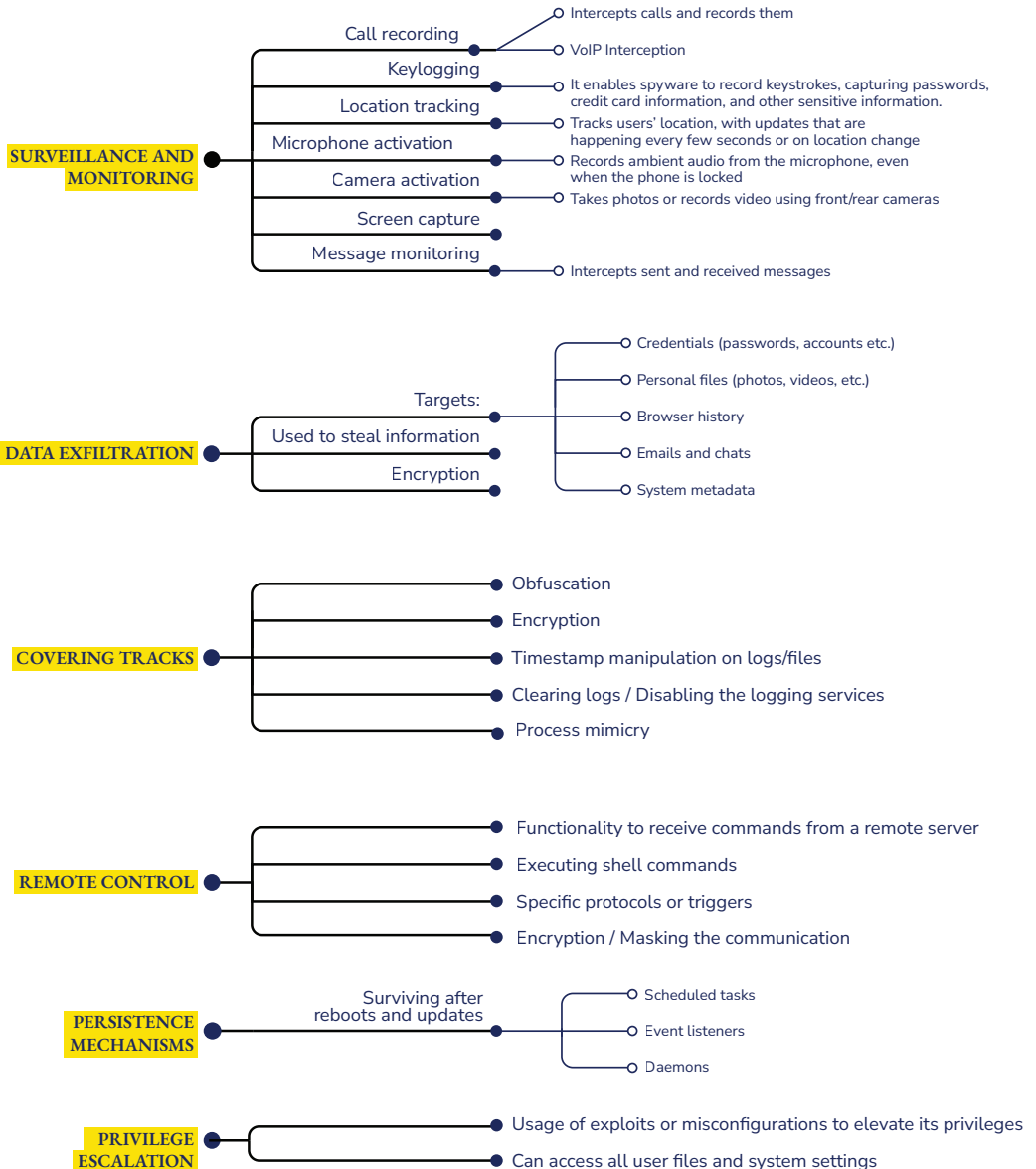
targeting political opponents and activists. One of the earliest documented cases dates back to 2012, when Bahraini pro-democracy activists were subjected to a FinSpy campaign uncovered by the Citizen Lab. The activists received emails posing as correspondence from an Al Jazeera journalist—complete with the reporter’s real name to enhance credibility. Attached archives contained malicious executables disguised as images and documents, using a “right-to-left override” trick common in scripts such as Arabic or Hebrew to conceal their true file type.

Once executed, FinSpy embedded itself deep within Windows processes, concealing its presence while creating hidden folders and harvesting a wide range of data. The spyware was capable of collecting screenshots, stealing passwords, recording Skype calls, and encrypting the exfiltrated information for transmission to its operators.³² Further investigations revealed FinFisher’s evolution beyond Windows. In 2020, Amnesty International documented a FinSpy campaign in Egypt that included versions developed for Mac and Linux – an unusual expansion, since most spyware kits historically focus on Windows and mobile platforms.³³

Analyses of today’s advanced spyware – such as Pegasus, Predator, and KingSpawn – show that their core functions remain broadly the same as earlier generations: recording audio, taking photos, tracking location, and exfiltrating data. What sets them apart is not new capabilities but the sophistication of the exploits they rely on. Pegasus, for instance, became infamous for its “zero-click” exploits, which allow infection without any interaction from the target.

These tools can also operate in parallel, compounding the threat. For example, forensic analysis of the phone of exiled Egyptian politician Ayman Nour revealed that it had been infected by both Predator and Pegasus simultaneously, deployed by two separate government clients. Investigators found four spyware-related processes running on his device, two linked to Predator and two to Pegasus, illustrating both the intensity of surveillance operations and the interoperability of commercial spyware.³⁴

A more recent and troubling capability of advanced spyware is the ability to “jump” from one app to others across a device. This was uncovered in the case of Paragon’s Graphite spyware, which was deployed against activists and journalists in Italy. Graphite uses an Android zero-click exploit chain that begins with a malicious PDF sent to a WhatsApp group where the target has been added by the attacker. When the file is delivered, WhatsApp automatically parses it, triggering the exploit. The Graphite implant is then loaded into WhatsApp, from which it breaks out of the Android sandbox and propagates into other apps on the device – vastly expanding its reach and potential for data extraction.³⁵



Compromising human rights and technical integrity

The proliferation of modern spyware tools has not only enhanced their methods of payload delivery and evasion of security mechanisms, but also expanded the range of capabilities once they infiltrate a device. While social engineering remains an important element of many successful spyware attacks,³⁶ the emergence of zero-click exploits has fundamentally shifted the landscape. For both the operators of these tools and their targets, the stakes are now dramatically higher.

Even those presumed to have strong awareness of cyber threats and rigorous operational security – such as investigative journalists, human rights defenders, or political dissidents – are not immune. If a device carries an unpatched vulnerability that is targeted with a zero-click exploit, infection is highly likely regardless of user vigilance. This does not render good digital hygiene or sound operational security meaningless; rather, it highlights how narrow the margin of safety has become. Even a minor lapse, such as postponing a mobile operating system update for a month, can create an opening with potentially severe consequences.

Modern mobile phones – smartphones – store an extraordinary range of information about their users and the people they interact with, reaching into the most intimate aspects of private life. Yet both dominant ecosystems, Google's Android and Apple's iOS, have made it increasingly difficult for ordinary users to safeguard their privacy, whether on the devices in their pockets or on the cloud servers that back them across the world. To make matters worse, the devices themselves – through their operating systems, built-in services, and the third-party applications users rely on – remain riddled with vulnerabilities. These weaknesses are exploited daily, leaving smartphones far from secure against the constant tide of breaches and attacks.

No matter how technically advanced it is, who the end-user may be, or how it is deployed, spyware remains malicious software because it compromises information systems – with all the implications that follow. These cyberweapons are among the most formidable threats not only to the technology that permeates our lives, but also to the protection of human rights and the principles of democratic governance. As with every intrusive technology, governments are reluctant to abandon or prohibit spyware and instead seek to justify its use through legal or political arguments. Yet

scandal after scandal – including in countries with relatively high levels of democratic development – demonstrates that the deployment of such intrusive tools is deeply problematic. Spyware attacks jeopardize a wide range of human rights, from privacy to freedom of expression, while also undermining the technical integrity of the software and hardware on which modern life depends. Only recently have technology companies whose products are targeted begun to respond in a more systematic way, by introducing stronger protective features and cooperating with organizations such as Amnesty International and Citizen Lab to patch vulnerabilities and publicize exploitation attempts.

As Google’s Threat Analysis Group (TAG) highlights in its Buying Spying report, “[...] spyware deployed against journalists, human rights defenders, dissidents, and opposition party politicians [...] has been well documented, both by analysis from Google, and by researchers from organizations like the University of Toronto’s Citizen Lab and Amnesty International. While the number of users targeted by spyware is small compared to other types of cyber threat activity, the follow-on effects are much broader. This type of focused targeting threatens freedom of speech, a free press, and the integrity of elections worldwide.”³⁷

THE “NEED” FOR SPYWARE

Outdated methods: How technological advancements rendered wiretapping (almost) obsolete

Until the mainstream adoption of smartphones around the 2010s, law enforcement agencies conducted investigations by intercepting communications – commonly referred to as ‘wiretapping’ – through established methods of monitoring analog and digital phone traffic, as well as so-called GSM³⁸ traffic. These communications and their associated metadata were centralized within the infrastructure of fixed and mobile network service providers, enabling relatively straightforward access for lawful interception.

Additionally, communications could be captured via man-in-the-middle (MITM) attacks, particularly through vulnerabilities in GSM protocols. For example, the A5/1 and A5/2 stream ciphers used in GSM encryption were susceptible to real-time decryption with modest computing power, and early IMSI-catchers (such as the Harris Corporation’s StingRay devices) exploited the lack of mutual authentication in GSM networks to intercept calls and SMS. These weaknesses made it possible to eavesdrop on mobile traffic without detection, especially before the widespread rollout of 3G and later LTE networks with improved encryption and integrity checks.

Since the early 2000s, state surveillance capabilities have undergone a radical transformation. While wiretapping – essentially a digital continuation of traditional eavesdropping – remained the primary technique even as telecom systems transitioned from analog to digital. Yet the post-9/11 era marked a decisive shift in priorities: intelligence and law enforcement agencies increasingly turned their attention away from the content of communications and toward metadata – information about who was communicating, when, for how long, and from where. Metadata soon proved more revealing, scalable, and easier to process than voice recordings or message content. Collected in bulk, often without attracting the same level of legal or public scrutiny, it became an indispensable tool for mapping social networks, tracking behavior, and tracing movement.

The typical legal and technical procedure involved a law enforcement agency (LEA) obtaining a court-issued warrant, which would then be presented to the relevant service provider (SP). In compliance, the SP would route the target's communications – such as fixed-line telephony, public phone booths, GSM mobile calls, SMS, and even mobile data – back to the LEA for monitoring. This process relied on the centralized control that service providers held over communications infrastructure.

In parallel, covert or unlawful interceptions were also technically feasible. Using techniques such as man-in-the-middle (MITM) or deep packet inspection (DPI), communications could be intercepted without the knowledge or cooperation of service providers. These approaches exploited protocol vulnerabilities and insufficient encryption to extract either content or metadata in transit.

However, this model began to break down with the widespread adoption of smartphones and the explosion of internet-based communication services. As voice and messaging services shifted toward decentralized platforms – such as VoIP providers, encrypted chat and video applications, and social media messaging – service providers no longer had access to the bulk of communication content. Compounding this challenge, many of these apps implemented strong end-to-end encryption, rendering traffic unreadable not only to ISPs but also to law enforcement and intelligence agencies operating within the infrastructure.

At this juncture, law enforcement agencies began to argue that traditional surveillance techniques had become ineffective. To overcome the barriers posed by encryption and decentralization, they sought new forms of access: either through cooperation from platform providers (often resisted or legally restricted), interception of traffic before encryption is applied, or most effectively, direct access to the device itself. This demand paved the way for the rise of targeted mobile device spyware – software capable of bypassing encryption altogether by capturing data at the source or destination, before it is encrypted or after it is decrypted by the device's operating system.

Beyond wiretapped content, another critical category of intelligence retained by service providers is communication metadata. Understanding how both

communication content and metadata are collected and accessed by LEAs requires a basic breakdown of mobile network architecture, particularly of how signaling, routing, and data storage interact across service layers.

MOBILE NETWORK ARCHITECTURE³⁹

Every commercially available smartphone uses the cellular network to support three basic types of traffic: voice calls, SMS, and mobile data. All are routed through the same core infrastructure, which means that the surveillance interception points are largely the same across these communication types.

To initiate any kind of communication, a mobile device identifies itself using two unique identifiers: the IMEI (International Mobile Station Equipment Identity), which identifies the device itself, and the IMSI (International Mobile Subscriber Identity), which is linked to the user's SIM card and mobile subscription. These identifiers are used during the authentication process to validate the device and subscriber within the mobile network.

Mobile operators deploy a geographically distributed network of Base Stations (BSs), which connect users' devices to the broader cellular infrastructure. These base stations link to the Mobile Switching Centre (MSC), which handles call setup, routing, and switching within the network. When a call is initiated, the originating device connects to the nearest base station, which relays the connection request to the MSC. The MSC then identifies and connects to the base station nearest to the receiving party to complete the call.

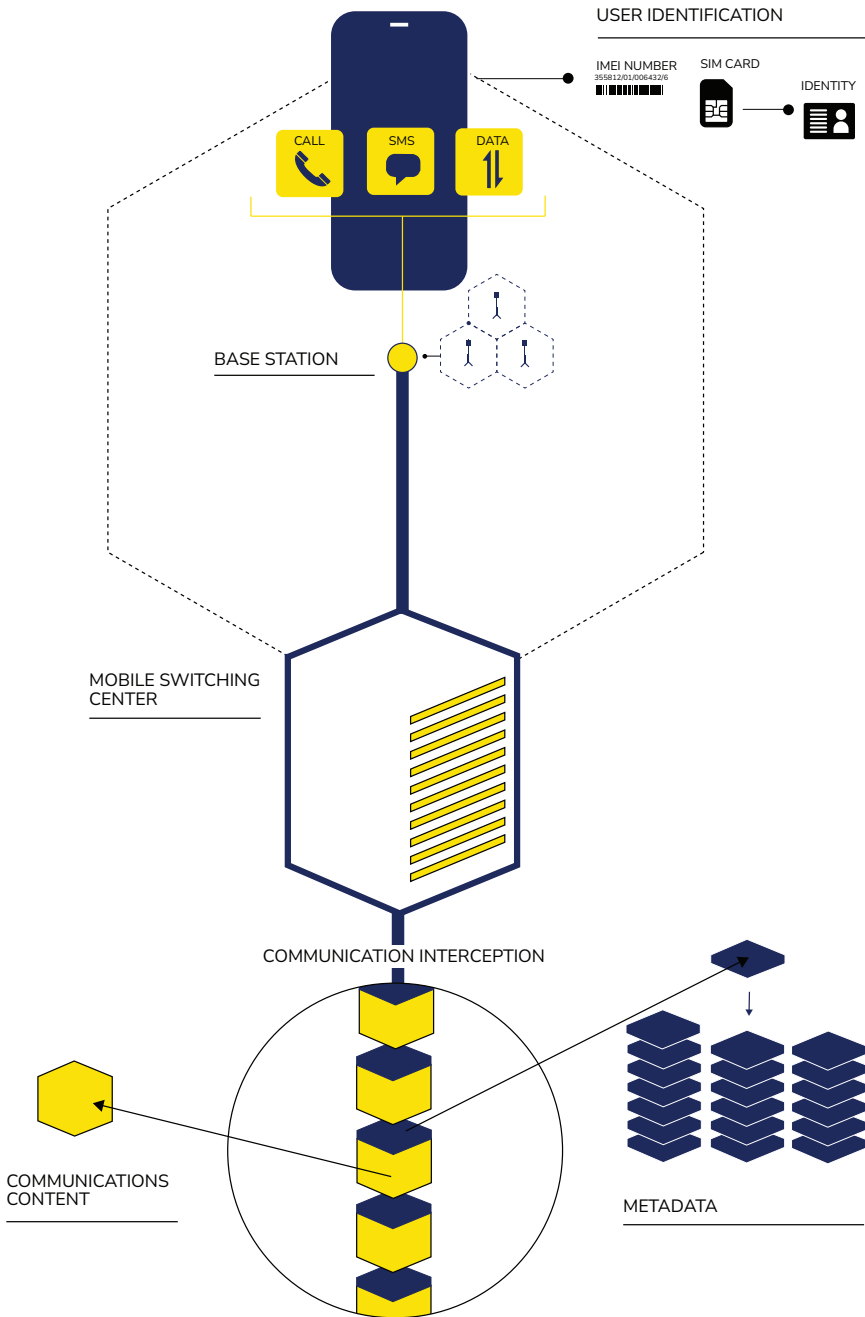
Once the call is answered and established metadata – including the identities of the caller and recipient (via IMSI or MSISDN), timestamp, duration, and location of the base stations involved – is generated and stored by the MSC. While the content of the call is transmitted through the MSC in real time, it is typically not stored by default, unless active interception or recording is triggered via legal or technical intervention.

In addition to the MSC, modern mobile networks include other key components relevant to surveillance, such as the Home Location Register (HLR), which maintains subscriber identity and location data, and the Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN), which handle packet-switched mobile data. These systems continuously generate metadata – such as cell tower locations, session durations, and IP addresses – that can be used to track user movements or reconstruct communication patterns. Most mobile carriers are also equipped with lawful interception (LI) interfaces, integrated into core network elements, which allow law enforcement agencies to access content and metadata in real time when authorized. These standardized interception points are specified by telecom regulations and industry bodies (such as ETSI in Europe), and their presence highlights how mobile network architecture is not only a technical system, but also a legally regulated space of surveillance.

WIRETAPPING

Wiretapping traditionally refers to the interception of telephone communications, often through technical access to telecom infrastructure or switching centers. While the term originally applied to analog lines, it later expanded to include digital calls, SMS, and certain forms of internet traffic. In most jurisdictions, wiretapping is legal only when conducted under judicial authorization, forming the basis of what is often referred to as “lawful interception”. Unauthorized interception – whether by individuals, criminal actors, or governments acting outside legal frameworks – constitutes a serious violation of privacy and communication rights.

In technical surveillance contexts, passive interception refers to monitoring communications without altering the traffic, such as listening to a call or reading transmitted data. Active interception, by contrast, involves manipulating or interacting with the communication stream, such as impersonating a network component (e.g. a fake cell tower) or injecting spyware. In wiretapping practice, most lawful surveillance is passive, whereas active methods are more common in offensive cyber operations or unauthorized espionage.



THE POWER OF METADATA: RETENTION AND ACCESS

The design of modern digital communication technologies inherently generates vast quantities of metadata – information about who talked with whom, when, from where, and through which services or applications. Metadata can also describe how users moved across digital environments, which websites or platforms they accessed, and for how long. This metadata is not a byproduct but a core component of how digital services function. It is systematically collected, retained, and monetized by companies, and increasingly accessed by government agencies for surveillance and law enforcement purposes. Often described as “data about data”, metadata defines and contextualizes the content it surrounds – but unlike content, it is typically unencrypted, easy to process, and legally less protected in many jurisdictions.

Although metadata does not capture the content of a message or call, it can often reveal more than the communication itself. Patterns of communication, frequency, location trails, and social graphs constructed from metadata can expose sensitive personal relationships, behavioral routines, political affiliations, religious practices, and even health conditions. In this sense, metadata is both highly revealing and difficult to falsify – it is often said that “metadata doesn’t lie”.

The collection and retention of metadata are governed by a patchwork of legal regimes, many introduced in the post-9/11 era and later revised to reflect digital transformations. In the EU, mandatory data retention mandates have been repeatedly invalidated by the Court of Justice of the European Union for infringing on fundamental rights. In Serbia, the Constitutional Court ruled in 2013 that key provisions of the Law on Electronic Communications were unconstitutional, as they allowed access to retained metadata without prior judicial approval, ignoring constitutional principles of protection and enabling access to retained data without a court decision.⁴⁰

Despite this decision, metadata access in Serbia remains opaque. Security and intelligence services continue to rely on broadly defined legal authorizations, and data retention is still practiced without clear public accountability.

Oversight mechanisms remain weak or procedurally fragmented, allowing retained metadata to be used both for targeted surveillance and broader monitoring purposes – without the transparency or safeguards necessary in a democratic society.

While metadata is most commonly obtained from service providers through formal or semi-formal channels, it can also be gathered through direct technical means. Certain surveillance tools were developed specifically to extract metadata from mobile devices without involving telecom infrastructure at all.

IMSI-CATCHER

One example of now-deprecated metadata-gathering technology is the IMSI-catcher. These devices exploited the cellular nature of mobile networks to simulate base stations and silently collect IMSI numbers (unique subscriber identifiers) from all phones within range. In some cases, they also enabled the interception of unencrypted traffic. While not wiretapping in the traditional sense, such tools allowed for passive mass surveillance – especially useful for identifying participants in protests or locating specific individuals.⁴¹ However, the increasing use of mutual authentication and encrypted communication has significantly reduced their effectiveness.

IMSI-catchers belong to a broader class of surveillance tools known as Cell Site Simulators (CSSs), which mimic legitimate base stations to trick nearby mobile phones into connecting. Once connected, the CSS can extract the IMSI (International Mobile Subscriber Identity) – a unique identifier tied to a SIM card – without the user’s knowledge. This identifier is intended to remain private, as it can be used to associate the device with its physical location, communication records, and online activity. CSSs exploit vulnerabilities in 2G (GSM) networks, which often lack mutual authentication and may allow unencrypted communication. Classic IMSI-catchers simply collect IMSI numbers and then release the devices, often by downgrading their connection from more secure 3G or 4G networks to 2G, or by jamming higher-frequency bands to force fallback. This process enables not only bulk identification but also location tracking, including “presence testing” (confirming whether a phone is in a given area) and more precise geolocation via trilateration or direct extraction of GPS data from the device. While modern encryption and mutual authentication

protocols have significantly limited the effectiveness of these tools, they remain emblematic of an era in which mobile network vulnerabilities were systematically exploited for surveillance without provider cooperation.

COMPUTING POWER AND THE RISE OF ENCRYPTION

One of the most important technological developments that rendered traditional wiretapping obsolete was the rapid increase in computing power. This enabled the rise of the smartphone market, which in turn accelerated decentralization of communication through mobile applications and internet-based messaging platforms. A few years later, this same computational capacity made widespread encryption technically feasible, even on personal devices. Because encryption is computationally intensive, its mass adoption was previously limited. Today, however, virtually all forms of communication and data storage can be, and often are, encrypted: chat messages, voice and video calls, emails, local devices, hard drives, cloud storage, websites, payment systems, and even data generated by Internet of Things (IoT) devices.

As a result, encryption has become a foundational technology for digital security, protecting not just information, but also personal identity, financial transactions, and the confidentiality of daily interactions. In this context, end-to-end encryption (E2EE) emerged as a critical evolution – designed to ensure that only the communicating parties can read the content, effectively locking out intermediaries, including service providers, internet infrastructure, and surveillance actors.

END-TO-END ENCRYPTION

This method ensures that data is encrypted on the sender's device and decrypted only on the recipient's. It is widely regarded as the most secure form of digital communication, as the data remains unintelligible to service providers, network operators, or any third parties during transit.⁴² Messaging applications like Signal and WhatsApp rely on end-to-end encryption (E2EE) to prevent unauthorized access to content.

The process typically follows four steps: encryption, transmission, decryption, and authentication. Encryption transforms plaintext into ciphertext using algorithms that rely on either symmetric keys (shared between sender and receiver) or asymmetric keys (a public key for encryption and a private one for decryption). The encrypted data then travels over the internet and is decrypted only at the endpoint, where authentication mechanisms – like digital signatures – verify the message's integrity and origin.

Signal, for instance, uses a custom cryptographic framework known as the Signal Protocol,⁴³ now adopted by WhatsApp and other platforms. Key features include forward secrecy (compromising a key doesn't reveal past messages), post-compromise security (future sessions re-secure themselves), and asynchronous secure messaging – a technically challenging yet critical function for real-world usability.

While this form of encryption is essential, it is not sufficient. It protects data in transit, but not the device itself. If a phone is infected with spyware, the attacker can access messages before they are encrypted or after they are decrypted, effectively turning secure communication into something akin to speaking in a glass room: protected from eavesdropping in transit, but still exposed, like someone reading your lips. Even the strongest encryption protocols cannot compensate for a compromised endpoint.

Beyond technical threats, political pressure continues to challenge encryption's integrity. One recurring demand is for encryption backdoors: built-in vulnerabilities intended to allow law enforcement access. As Apple's CEO Tim Cook warned in 2015, you can't have a backdoor just for the good guys.⁴⁴ A system weakened by design is vulnerable to anyone, including malicious actors.

Today, governments rarely ask for backdoor keys. Instead, they invoke broad narratives of safety, crime prevention, and national security to justify targeted surveillance, often using commercial spyware. This shift reflects a strategic pivot: rather than breaking encryption, many authorities now seek to bypass it entirely by compromising the device itself.

The encryption illusion

A persistent myth among civil society members claims that using secure messaging apps like Signal offer complete protection simply because of their strong encryption protocols and reputation for resisting data sharing with law enforcement. While Signal's cryptographic design is robust, no app – no matter how well-encrypted – is immune to spyware that operates directly on the device, capturing content by taking screenshots or logging keystrokes, without ever needing to intercept or decrypt network traffic.

Some messaging and banking apps have introduced anti-screenshots features, but these protections are often ineffective against spyware, which typically has elevated privileges that bypass interface-level restrictions.

More fundamentally, adoption remains inconsistent. Despite the availability of secure tools, many activists and journalists in high-risk environments continue to use unencrypted channels, leaving their communications vulnerable to interception. Others neglect to use basic obfuscation tools, such as VPNs or Tor, that could mitigate metadata exposure and location tracking. Without broader digital hygiene practices, even strong encryption can provide only a false sense of security.

INFECTION PROCESS

Every lock has a key – or, failing that, a way to open it without one. For locksmiths and lockpickers alike, the essential skill lies in understanding how each lock works. With spyware, the situation is similar: to develop an effective tool, vendors must possess extensive technical knowledge, which they use to discover vulnerabilities, craft exploits, and deliver spyware agents – the malware that compromises information systems.

The more widespread the targeted product, the greater the risk such vulnerabilities pose. A flaw in Windows, Google Chrome, or iMessage is far more dangerous – and valuable – than one in less common software or hardware. This demand has created a lucrative market for vulnerabilities, where researchers or hackers can sell their discoveries to the highest bidder.⁴⁵

According to Google’s Threat Intelligence Group (GTIG), Chrome was the primary focus of zero-day exploitation among browsers in 2024, while exploit chains leveraging multiple zero-day vulnerabilities were almost exclusively directed at mobile devices.⁴⁶

The spyware infection process is complex, often involving multiple stages and exploits to leverage vulnerabilities, compromise a device, and gain access to both stored information and its functionalities (camera, microphone, etc.). Understanding this process is critical for preventing and mitigating spyware attacks, whether from the perspective of vendors building defenses, individuals who may be targeted, or researchers working to uncover and expose cyber-espionage.

ATTACK STAGES

From the initial targeting to full control of a device, spyware attacks follow a structured sequence of stages.

Targeting and exploit delivery

The first stage of infection is identifying and reaching the intended device, presumed to be in the target’s use. Modern messaging platforms such as WhatsApp or Viber, which require an active phone number for registration, have become common channels for delivering malicious payloads. Law enforcement and intelligence agencies – the primary clients

of advanced spyware – often obtain target phone numbers through mandatory communications data retention regimes or SIM card registration requirements, making it easy to link a number to its user. Mobile network operators also store IMEI numbers, unique identifiers tied to each device model, which can give attackers additional technical insight and improve the precision of their targeting.⁴⁷

As we will explain further, targeting can be carried out remotely through one-click attacks based on social engineering, such as tricking the targeted individual into clicking a link or opening an attachment. More advanced zero-click exploits require no interaction at all – a malicious message or file is enough to initiate infection. Another form of remote attack operates at the mobile network level, where network equipment (“middleboxes”) can be used to redirect a target’s internet traffic to malicious domains hosting spyware, enabling the injection of the payload.⁴⁸

Finally, some spyware, such as the so-called NoviSpy Android spyware identified in Serbia,⁴⁹ is deployed through direct physical access to the device – typically during detention, arrest, or seizure, when the owner is unable to intervene. In such cases, installation may rely on specialized forensic tools, such as Cellebrite’s UFED, which can bypass screen locks and encryption to enable the planting of spyware.

Exploitation of vulnerabilities

As noted earlier, spyware attacks rely on exploits – technical tools designed to take advantage of software vulnerabilities and clear the way for spyware agents. According to Amnesty International, “on modern mobile devices exploits must bypass numerous layered security defenses and can be highly complex. A full exploit chain targeting latest device versions can sell for millions of Euros.”⁵⁰

Exploits typically operate in sequence, peeling away one layer of security after another until spyware implants can be installed. Because both iOS⁵¹ and Android⁵² now include multiple layers of protection against unauthorized access and tampering, these exploits must be exceptionally sophisticated.⁵³ Their ultimate goal is often to obtain root access, granting attackers unrestricted control over the device’s resources and commands.

In general, exploits used by advanced spyware tools fall into three main categories: remote code execution (RCE), sandbox escape, and local privilege escalation.⁵⁴ Remote code execution allows attackers to run malicious code on a target system from a distance, for example by exploiting a buffer overflow, where an application is forced to write more data into memory than it can handle, enabling the injection of malicious code.⁵⁵ Sandbox escape, in turn, targets the mechanisms designed to isolate applications and restrict their impact; by exploiting weaknesses in the sandbox, attackers can break out of this controlled environment and gain broader access.⁵⁶ Finally, privilege escalation enables the attacker to elevate their rights within the system, effectively becoming a system administrator or root user and obtaining unrestricted control.⁵⁷ Without these types of exploits working in sequence, spyware as an unknown or potentially malicious application would remain confined by protections like those built into iOS and Android, unable to fulfill its purpose.

Spyware agent installation

Once exploits have successfully leveraged device vulnerabilities, spyware agents are installed with the goal of compromising both stored information and core device functions, such as audio recording or camera control. With root access obtained through the exploit chain, the attacker effectively gains unrestricted control over the system, allowing the spyware to operate at its full capacity.

However, the inner workings of a spyware agent can also be highly complex, as demonstrated by Predator, an advanced tool sold by the Intellexa Group. Technical analysis of a Predator sample for Android revealed that it operates in tandem with another component known as Alien.⁵⁸ While it is common for sophisticated malware to rely on a “loader” – malware designed to deliver additional payloads once a system is compromised,⁵⁹ Alien plays a more integral role. In addition to downloading and updating Predator, Alien helps bypass Android security features, reads and executes code from designated locations, collects device and system information to map directories, and gathers configuration data.⁶⁰

Information gathering and exfiltration

Once successfully planted and installed, spyware agents initiate background processes that remain invisible to the user, who continues to operate their device as usual – exactly as the attackers intend. These processes allow

the spyware to access chat messages, emails, call logs, contacts, photos, videos, and more. It can also track location, take screenshots, activate the microphone, record calls, or capture photos and video through the camera. While the device is connected to the internet, this information is transmitted to an attacker-controlled command-and-control (C2) server, which can also issue instructions to manipulate the device and exploit its functions. To remain undetected, spyware may be configured to minimize suspicious behavior – for example, by exfiltrating data only over Wi-Fi connections to avoid unusual spikes in mobile data traffic.

ATTACK SURFACES AND VECTORS

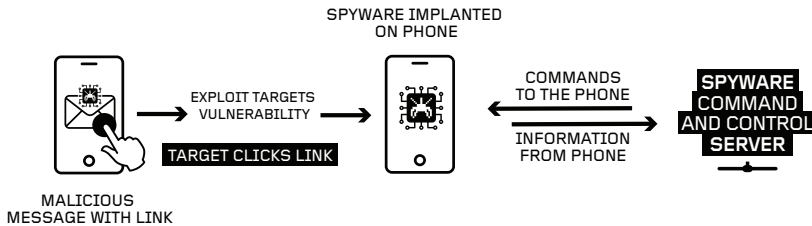
When analyzing spyware, it is important to distinguish between *attack surfaces* and *attack vectors*. In simple terms, the attack surface represents the breadth of potential entry points into a system, while attack vectors are the concrete methods used to exploit them.

An attack surface includes all possible points where an unauthorized user can access a system and extract data, whether physical or digital.⁶¹ A larger surface means more opportunities for exploitation. The digital attack surface covers all software-based points that can be targeted remotely or locally, such as operating system vulnerabilities, applications, code, ports, servers, or websites. By contrast, the physical attack surface encompasses devices that an attacker can physically access, including laptops, USB flash drives, hard drives, and mobile phones.

On the other hand, an attack vector is the specific method or pathway used to gain unauthorized access through one of the points on the attack surface.⁶² Common vectors include phishing, malware delivery, compromised passwords, or exploiting unpatched software.

In short, the attack surface represents where an attack could take place, while the attack vector represents how it is carried out. Minimizing the attack surface and defending against known vectors are both essential for mitigating digital security threats, including spyware. The following section outlines several common remote spyware attack vectors (one-click, zero-click, and network injection), as well as the physical access vector.

One-click remote attacks



One of the most common avenues for cybercrime and cyberspies is social engineering. As hacker and researcher The Grugq once tweeted: “Give a man an 0day and he’ll have access for a day, teach a man to phish and he’ll have access for life.”⁶³ This cybersecurity twist on a familiar saying underscores how valuable social engineering can be in an attacker’s arsenal – often more so than a single rare vulnerability.

In essence, social engineering is “the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust”.⁶⁴

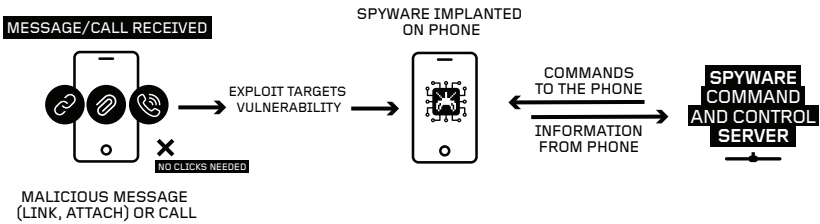
When it comes to spyware delivery, widely used messaging apps such as WhatsApp, iMessage, or Viber are among the most common vectors for targeting individuals with advanced spyware. Their ubiquity among users – particularly high-risk groups like journalists, activists, attorneys, politicians, and state officials – combined with limited privacy controls, makes them especially effective channels for spyware deployment. For example, registering for services such as WhatsApp, Viber, or Telegram requires nothing more than an active phone number, lowering the barrier for attackers to connect identities with devices.

The idea behind these delivery methods is to draw the target into a psychological game, using manipulation to prompt them to click on a malicious link or open a compromised attachment. Depending on the profile of the target, such messages are often crafted around highly sensitive themes – for instance, alleged evidence of human rights violations,

government corruption, or abuses of power – to maximize the likelihood of engagement.

Social engineering-based spyware attacks are often highly context specific. A notable case occurred in February 2025, when two investigative journalists in Serbia were targeted with Pegasus. Both received Viber messages from an unknown Serbian (+381) number at roughly the same time. The messages, written in Serbian and containing a link with a Serbian-language domain, read: “do you have info that he is next?” – a phrase carefully chosen given the wave of arrests for alleged high-level corruption then unfolding across the country, a topic of direct relevance to investigative journalists. Viber, being one of the most widely used messaging apps in Serbia, was deliberately chosen over alternatives such as WhatsApp. Although the journalists did not click on the link, subsequent analysis by Amnesty International’s Security Lab confirmed that it was a Pegasus infection attempt, which redirected to a decoy page of N1, a Serbian media outlet.⁶⁵

Zero-click attacks



In addition to one-click exploits, which depend on social engineering and user interaction, an even greater threat comes from zero-click attacks. These exploits are named for the fact that they require no action from the targeted individual: simply receiving the malicious communication is enough to trigger the infection. A zero-click attack succeeds when an exploit leverages an unpatched vulnerability, something especially likely if a device has not been updated for a long time or if it is an older model no longer receiving critical security patches. Like one-click exploits, zero-click attacks can be

delivered through messages or calls, but their effectiveness depends entirely on the underlying hardware or software vulnerabilities being targeted.

In 2023, Amnesty International forensically analyzed the phones of two Indian journalists targeted with a Pegasus iOS zero-day exploit known as BLASTPASS. According to their findings, the exploit unfolded in two stages. The first involved interaction with Apple's HomeKit service, which is used to control smart devices. In the second stage, attachments with the .pkpass file type were delivered via iMessage. On the iPhone of journalist Anand Mangnale, investigators found numerous traces of HomeKit service crashes, followed by files named sample.pkpass. These files contained embedded images that were automatically parsed by the device, requiring no user interaction. The images, however, carried malicious payloads designed to achieve remote code execution. Whether these exploits ultimately succeeded in infecting Mangnale's phone with Pegasus remained unclear.⁶⁶

Another example of an iOS zero-click exploit campaign was uncovered by Kaspersky researchers while monitoring network traffic on their corporate Wi-Fi network.⁶⁷ Dubbed *Operation Triangulation*, the campaign employed a highly complex exploit chain involving four zero-day vulnerabilities. The attack began with the delivery of a malicious PDF attachment via iMessage and proceeded to exploit multiple layers of Apple's architecture: an Apple-specific TrueType font instruction, the Safari browser, and finally two kernel vulnerabilities.⁶⁸ This chain represented one of the most sophisticated spyware zero-click and zero-day operations observed in the wild, and it prompted extensive follow-up research within the cybersecurity community.

Remote attacks via network infrastructure

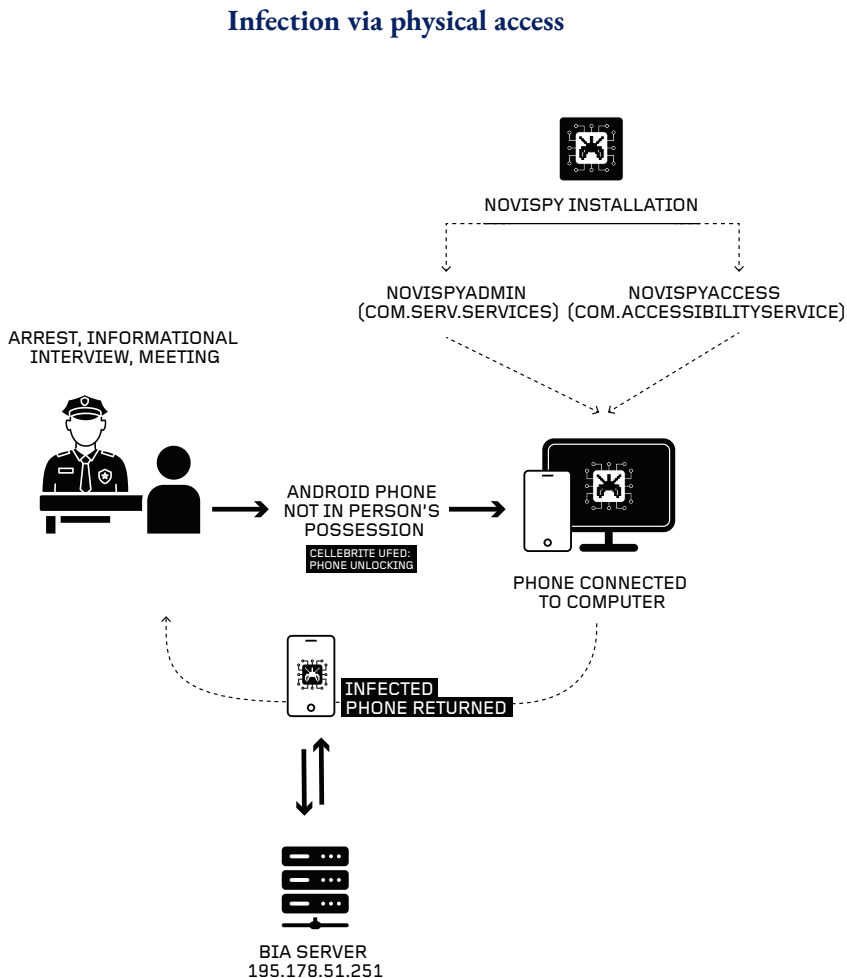
Another spyware delivery mechanism involves exploiting mobile network infrastructure, where specialized equipment is installed to control internet traffic and inject malicious payloads. In such cases, it is generally assumed that network operators cooperate with government bodies, since operators hold subscriber information that governments may want to target. While this method appears less common than other remote spyware delivery techniques, it has been reported in countries such as Turkey and Egypt. In 2018, for instance, spyware was injected in Turkey and Syria when users attempted to download popular software installers (e.g., Avast Antivirus, CCleaner, WinRAR) from legitimate websites. Instead of receiving the

expected software, users were redirected to malicious traffic that delivered spyware. This was possible because some legitimate sites – such as Download.com – failed to automatically redirect visitors to secure HTTPS versions, leaving them vulnerable on unencrypted HTTP pages where attackers could serve spyware in place of genuine installers.⁶⁹

A similar method was used to deliver Predator in Egypt in 2023, when the phone of Egyptian politician Ahmed Eltantawy was persistently targeted with network injections. Between Telecom Egypt and Vodafone Egypt (Eltantawy’s provider), a “middlebox” device was deployed to inject spyware. When Eltantawy visited HTTP websites on Vodafone’s mobile network, his connection was silently redirected to a page containing two embedded code elements – one delivered a benign file, while the other was an invisible element carrying a Predator infection link. Based on their prior research, Citizen Lab determined with high confidence that the device used to manipulate mobile traffic was Sandvine’s PacketLogic.⁷⁰ In early 2024, in the aftermath of these findings, the US Department of Commerce placed Sandvine on an export blacklist for its products’ role in internet censorship and spyware attacks in Egypt.⁷¹

When it comes to Predator, recent research has revealed a range of Intellexa Alliance products designed to deliver the spyware through either strategic or tactical zero-click infections, similar to the network injection methods described above. Strategic infections are carried out via internet service providers (ISPs). For this purpose, Intellexa markets two products: Mars, which redirects HTTP connections, and Jupiter, an add-on to Mars that enables redirection of encrypted HTTPS connections, but only for websites hosted with an ISP in the target’s country.⁷²

For tactical infections, which require physical proximity to the target, Intellexa offers Triton, a tool that exploits vulnerabilities in Samsung devices’ baseband software and can be deployed within a range of “up to hundreds of meters”. Another product line, SpearHead, provides Wi-Fi interception capabilities and can be used for target identification, geolocation, traffic interception, and spyware injection. SpearHead systems come in multiple variants – they can be carried in a briefcase, mounted on a drone, or installed in a van.⁷³



When a targeted device is physically in the hands of a threat actor, installing spyware with the right tools becomes a relatively straightforward process. Situations such as detentions, arrests, or so-called “informational interviews” provide opportunities for devices to be confiscated and temporarily out of their owners’ reach. Documented cases show that authorities in Serbia, Russia, and China have used spyware that relies on direct access installation.

Before examining direct installation spyware modules, it is important to highlight the role of digital forensics tools such as Cellebrite's UFED devices⁷⁴ in the infection process. Widely used by law enforcement agencies around the world, Cellebrite's products have become synonymous with device unlocking, data extraction, and forensic analysis. In cases where phone passcodes are unknown or owners refuse to disclose them – as documented in Serbia – Cellebrite tools have been identified as “spyware's first step”.⁷⁵

UFED devices rely on sophisticated zero-day exploits to take advantage of vulnerabilities in mobile operating systems. For instance, Amnesty International, in collaboration with Google, discovered an Android privilege escalation vulnerability on the phone of a Serbian activist that had been exploited through UFED. The flaw, which affected devices using Qualcomm chipsets, potentially exposed millions of phones before Qualcomm issued a patch in October 2024.⁷⁶

Cellebrite's effectiveness also depends on the state of the device. Phones in an After First Unlock (AFU) state – powered on and previously unlocked – hold system encryption keys in memory, making it easier to access and extract data. By contrast, Before First Unlock (BFU) phones remain more resistant to extraction. In some cases, UFED tools can also attempt brute force attacks to recover passcodes and encryption keys.⁷⁷

Cellebrite UFED devices support companion software called Inseyets, which provides advanced data access and extraction capabilities. This software works in tandem with a “Turbo Link” adapter, to which a target device is physically connected. Once attached, the system deploys a range of techniques and exploits to unlock the device and bypass security protections.⁷⁸

One unlocking method uncovered during the forensic analysis of a student activist's phone in Serbia involved a previously unknown zero-day exploit chain targeting Android USB kernel drivers. Because the vulnerability was not tied to a specific vendor or model, it potentially affected more than a billion Android devices worldwide. Cellebrite's toolkit exploited this weakness by emulating various external USB device types – such as webcams or mice – in order to trigger flaws in the Linux kernel and ultimately gain root-level code execution.⁷⁹

In February 2025, Cellebrite announced it would cease providing its products to customers in Serbia – most likely the police and the Security Information Agency (BIA) – after reports of misuse against journalists and activists were detailed in Amnesty International’s December 2024 findings.⁸⁰

In December 2024, Amnesty International reported that Android phones belonging to journalists and activists in Serbia had been infected with a spyware kit dubbed NoviSpy. Presumed to be domestically developed, this module was covertly implanted after the phones were unlocked with Cellebrite’s tools or by other means, and then directly connected to a computer. The attackers enabled developer mode – a feature intended for software testing that lowers the device’s security defenses – and issued commands through Android Debug Bridge (ADB). This process disabled key safeguards such as Google Play Protect, clearing the way for malicious applications like NoviSpy to be silently installed.⁸¹

The NoviSpy module consists of two malicious Android applications, or APKs, named NoviSpyAdmin and NoviSpyAccess. The Admin app is designed to request sweeping permissions, including administrative access to highly sensitive features, which enables it to retrieve call logs, contacts, SMS messages, and even record audio through the microphone. The Access app, by contrast, exploits legitimate Android accessibility features to capture screenshots, exfiltrate the data, track the device’s location, and activate the camera for recording. Both apps were found communicating with servers linked to Serbia’s Security Information Agency (BIA) and the state-controlled telecom provider Telekom Serbia, strengthening the attribution of NoviSpy to Serbian government entities.⁸²

Further analysis of the NoviSpy apps by SHARE Foundation revealed that NoviSpyAdmin communicated with a remote server via FTP (File Transfer Protocol) and could also respond to SMS commands. To encrypt the data it collected, the app used the Advanced Encryption Standard (AES); however, the encryption key was hardcoded into the application, representing a serious design flaw. NoviSpyAccess appeared more sophisticated: it used the Tor network to anonymize communications and relied on the ADB protocol to execute shell commands remotely. It also implemented a custom version of AES encryption, both to secure the exfiltrated data and to conceal its activity on the device.⁸³

Another case of spyware installed through direct device access was documented in Russia, where a malicious version of a legitimate Android application was planted on the phone of Russian programmer Kirill Parubets, accused of sending money to Ukraine. His phone was seized during a search of his apartment, and he was beaten until he revealed the device passcode. The spyware masqueraded as Cube Call Recorder, a genuine app available on the Google Play Store, but requested far more invasive permissions than the original. It operated in two stages, with the second stage enabling malicious capabilities such as file and password extraction, keylogging, execution of shell commands, and more. Code references to iOS within the application suggested that an iPhone version might also exist.⁸⁴

Finally, a surveillance tool known as EagleMsgSpy was found to be used by public security bureaus in China. The spyware consists of two components – an APK installer and a client application that runs on the device. While its primary focus appears to be Android, internal documents and source code suggest that an iOS version may also exist. Installation can be initiated either by scanning a QR code or via a USB connection. Once active, operators can manage the spyware through a web-based administration panel, which provides access to details about targets such as their 10 most frequently contacted individuals and geographical heatmaps of those contacts, as well as capabilities for real-time audio recording and photo collection.⁸⁵

COMMUNITY AND INDUSTRY RESPONSES

Resilience against spyware attacks today depends heavily on a broad community of technologists, investigators, computer engineers, hackers, and civil society organizations that dedicate their efforts to understanding and exposing these threats. Their work, however, is only as strong as the communication and collaboration they establish with industry actors – device manufacturers, operating system developers, and app providers whose products are exploited by spyware.

Most of what is known about how spyware functions comes from forensic analysis of infected devices and reverse-engineering of malicious applications. This process requires a high degree of trust between people affected and civil society organizations, since consensual forensic work often involves access to highly sensitive personal information such as chat logs, photos and videos, browsing and location history, and more.

Equally critical is the cooperation between civil society actors and major technology companies such as Google and Apple, whose security teams play a central role in detecting malicious activity and notifying targets. Because so much data flows through their platforms and infrastructure, these companies remain indispensable partners in both uncovering attacks and mitigating their impact.

Detection

Identifying spyware is a critical step in mitigating its harmful effects. Since these tools are designed to operate silently in the background, without alerting the user, they can often remain undetected for long periods. This makes discovery particularly challenging on smartphones, where unusual performance issues or increased network usage can easily be mistaken for normal behavior.

To uncover spyware, researchers rely on several methods to detect signs of suspicious activity on a device. The four most commonly used approaches are:⁸⁶

- » Static method – analyzes a suspicious program without executing it. Malicious components are extracted and a digital “fingerprint” is created (e.g., byte patterns, strings, or hashes). These fingerprints are later compared against databases of known patterns; a process often referred to as signature-based detection.
- » Dynamic method – observes how the program functions when running. This approach looks at the spyware’s behavior in real time, using models trained on past data to detect suspicious activity during execution.
- » Hybrid method – combines static and dynamic techniques. It begins with static analysis, then follows up with behavioral checks to confirm whether spyware activity is present.
- » Machine learning method – uses algorithms trained to classify activity as spyware-related or benign. These models learn from large datasets containing both real-world spyware samples and simulated behaviors, enabling them to spot new or evolving threats.

Community responses

Mobile Verification Toolkit (MVT)

Developed by Amnesty International’s Security Lab in July 2021, MVT is designed to support consensual forensic analysis of Android and iOS devices by identifying traces of compromise.⁸⁷ The release of the toolkit was accompanied by a technical forensic methodology, published as part of the Pegasus Project.

It works with Indicators of Compromise (IOCs) – digital forensic artifacts such as IP addresses, domain names, or file hashes that signal a potential breach or malicious activity on a system or network. By using IOCs published by Amnesty International and other research groups, the toolkit can scan mobile devices for traces of targeting or infection linked to known spyware campaigns.

Public IOCs allow independent researchers to make an initial assessment of a device, while also fostering community analysis, faster response during active campaigns, and providing learning material for new investigators on how spyware behaves in real-world cases. However, once such indicators are disclosed, attackers often change their infrastructure, quickly rendering them obsolete. For this reason, public IOCs are not sufficient to conclude that a device is “clean” or has not been targeted by a particular spyware tool. Relying on them alone can overlook recent forensic traces and create a false sense of security.

Reliable and comprehensive digital forensic support and triage require access to non-public IOCs, research, and threat intelligence. Using private indicators can help identify new variants of spyware, as attackers usually do not change their infrastructure immediately. However, it takes time for this information to be disseminated and acted upon, even among those capable of conducting such research, such as NGOs and journalists.

Android Quick Forensics (AndroidQF)

Another useful tool for investigators is AndroidQF, which enables the rapid collection of forensic evidence from Android devices to help uncover potential traces of compromise.⁸⁸ It automatically gathers key data such as installed apps, contact lists, SMS and call history, event logs, and user accounts. The tool prioritizes non-system applications and excludes trusted apps to streamline the analysis. Once the data is collected, it can be processed with MVT against known IOCs, such as package names or certificate hashes. This approach has proven especially effective in detecting NoviSpy spyware,⁸⁹ along with other malicious APKs.

GrapheneOS

A privacy- and security-focused mobile operating system built on the Android Open Source Project (AOSP), it introduces significantly hardened defenses compared to standard Android.⁹⁰ Key features include:

- » Enhanced exploit mitigations – stronger defenses against common attack methods.
- » Stricter app sandboxing – tighter separation between applications
- » No Google services by default – reducing exposure to data collection.

- » Secure application permissions – more fine-grained control over what apps can access.

GrapheneOS is supported on select Google Pixel models, starting from the Pixel 6 series, and offers a strong option for users seeking maximum control over their data and device security.

Industry spyware mitigation

Both Google and Apple take proactive measures to combat modern spyware threats on their operating systems.

Apple maintains a tight grip over both hardware and software, which enables strong security across its ecosystem. Because iOS runs exclusively on Apple devices, the company has full control over system updates, security policies, and the app marketplace. This allows Apple to deliver updates and security patches universally to all supported devices – often for 5 to 6 years after release.⁹¹

In contrast, Android is an open-source operating system developed by Google and licensed to many manufacturers, each of whom can implement it differently. While Google controls the Android core, it does not have full authority over how and when devices receive updates, which can delay the patching of vulnerabilities. Most Android manufacturers still provide only 2 to 3 years of major OS updates and 3 to 4 years of security patches.⁹²

However, things have been improving, as both Google and Samsung have made significant progress. Google's Pixel devices, starting with the Pixel 8, now promise a full 7 years of OS and security updates – setting a new standard for the Android ecosystem.⁹³ Not to be left behind, Samsung has extended support to 4 years of OS updates for many of its phones, and up to 7 years of updates for higher-end models, beginning with the Galaxy S24 series.⁹⁴

Apple and Google have also introduced threat notifications to alert and assist users who may be individually targeted by spyware. Apple began sending such notifications more publicly in late 2021, following the discovery of high-profile spyware like NSO Group's Pegasus.⁹⁵ When Apple detects activity consistent with a state-sponsored attack, users receive a warning via email and iMessage, though the company keeps most technical details of the attack confidential.

Google, on the other hand, takes a broader approach. Its Threat Analysis Group (TAG) monitors not only Android but also Gmail, Chrome and Google Drive.⁹⁶ When TAG identifies a potential threat, users are alerted, typically through email and in-browser notifications.⁹⁷ Like Apple, Google does not disclose the specific methods it uses to detect these attacks, in order to avoid giving attackers information that could help them adapt.

When it comes to anti-spyware measures, Apple has introduced features such as BlastDoor⁹⁸ and Lockdown Mode.⁹⁹ BlastDoor, rolled out in iOS 14, was designed to protect iMessage from zero-click exploits. Before its introduction, vulnerabilities in how iMessage processed attachments such as images and PDFs had been abused to install spyware. Lockdown Mode, introduced in iOS 16, is aimed at high-risk users such as journalists and activists. It significantly reduces the attack surface by disabling certain features, applications and websites.

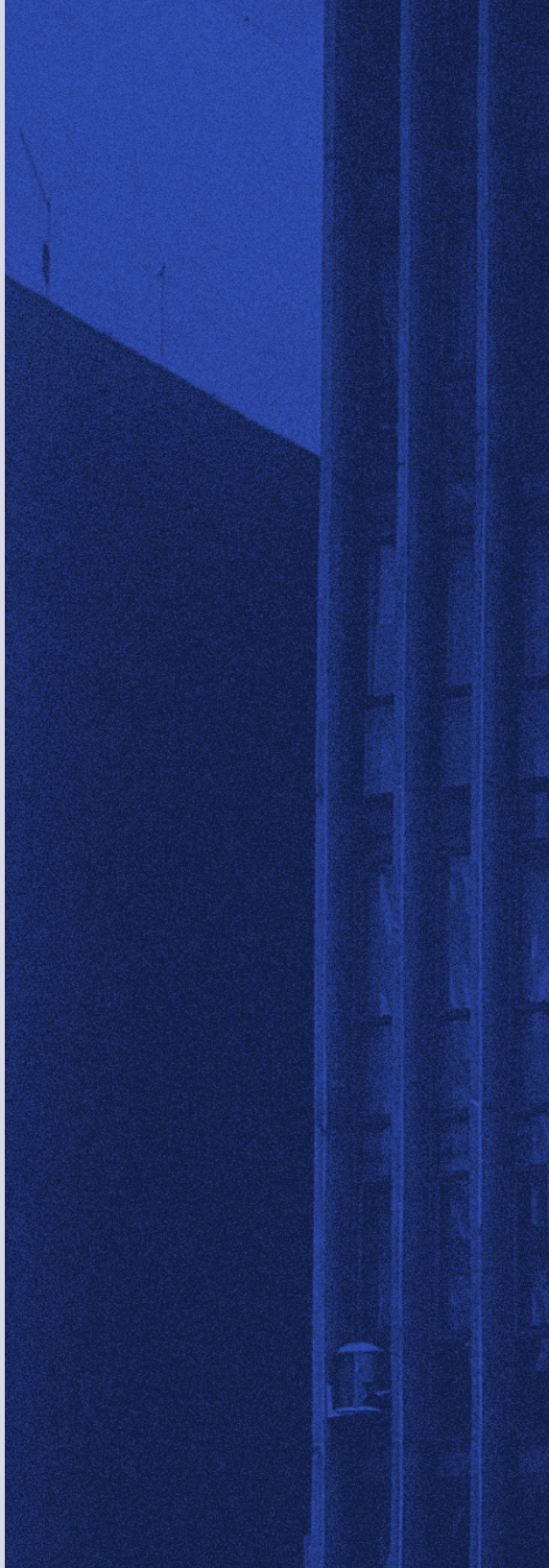
Meanwhile, Google has integrated Google Play Protect into Android, which scans more than 100 billion applications each day to detect malware.¹⁰⁰ To address delays in patching, Google introduced Project Mainline with Android 10, enabling core security components to be updated directly through the Play Store, bypassing manufacturers.¹⁰¹ More recent versions, Android 13 and 14, expanded privacy and security with more granular permission controls and runtime notifications for clipboard access and background activity. Looking ahead, Android 16 is expected to include an Advanced Protection Mode – similar in concept to Apple’s Lockdown Mode – designed specifically for high-risk users.¹⁰²

Google also issues the Android Security Bulletin on a monthly basis and contributes to the wider security community through Project Zero, its dedicated team that investigates and discloses zero-day vulnerabilities.¹⁰³

Samsung, as the largest Android device manufacturer, plays a distinctive role. While it relies on Google for the base OS, Samsung enhances security with Knox, a hardware-backed platform designed for both consumers and enterprises.¹⁰⁴ Knox includes features such as real-time kernel protection, secure boot and containerization of apps and data.

Meta, through WhatsApp, also works to counter spyware by relying on end-to-end encryption, proactive threat monitoring and user alerts.¹⁰⁵ The platform notifies users who may be at risk and collaborates with research groups such as Citizen Lab.

A PRIVACY NIGHTMARE: UNDERSTANDING SPYWARE





LEGAL

LEGAL

Spyware has emerged as one of the most dangerous and intrusive surveillance technologies of our time. It allows invisible and unrestricted access to a person's private life, including their communications, movements, thoughts, and relationships, without their knowledge. Despite its vast potential for abuse and the serious threat it poses to fundamental rights, there is currently no comprehensive legal framework, either at the national or international level, specifically regulating spyware. With only a few exceptions, spyware continues to operate in a legal grey zone, even as its development and use by both state and private actors rapidly expands.

This legal vacuum creates a deeply troubling situation. Rather than strengthening legal protections, some states are moving toward normalizing the use of spyware through overly broad legal authorizations, often justified in the name of national security or crime prevention. Such developments risk legitimizing a tool that, by its nature, violates core principles of necessity and proportionality under international human rights law. Even in the investigation of serious crimes, the use of spyware cannot be justified when less intrusive means are available. The level of surveillance enabled by spyware is fundamentally incompatible with the right to privacy, the presumption of innocence, and the integrity of democratic society.

Accordingly, this part of the study focuses on how existing laws fail to adequately address the dangers of spyware and why its use must be rejected as unlawful. The analysis takes a country-by-country approach, applying a consistent legal framework that covers the following key categories: the right to privacy, protection of personal data, confidentiality of electronic communications, confidentiality of digital devices, spyware in criminal legislation, special investigative measures, and privacy in the context of digital surveillance.

APPROACH AND METHODOLOGY

In most of the countries examined in this study, the use of spyware is not explicitly regulated by law. As a result, our approach has been to assess the broader legal and constitutional frameworks that may indirectly affect the legality or practical feasibility of deploying such intrusive technologies. The assumption is that if a country has strong constitutional or legislative protections for the right to privacy and personal data – and if these rights are supported by robust enforcement principles – then the legal space for the use of spyware is likely to be significantly limited. Furthermore, if a legal system prohibits activities such as the development, distribution, or use of computer viruses or similar technologies, and does not explicitly carve out exceptions permitting spyware for narrowly defined lawful purposes, we infer that its use would be considered unlawful. Accordingly, the study also examines more general legal provisions, not to suggest that they directly regulate spyware, but to draw conclusions about its legal status by implication, in the absence of express regulation.

In line with this approach, the following part of the study presents a comparative legal analysis of a range of countries with different legal and political systems. The analysis is structured around seven thematic sections, operationalized through a mixed-method questionnaire. This methodology builds on our earlier work on the legality of spyware in Serbia, which involved an in-depth examination of Serbian law. Using the same legal reasoning and human rights standards as a generalized conceptual framework, we designed the questionnaire to assess comparable legal standards regarding spyware in other jurisdictions.

The questionnaire was distributed to legal experts in each of the selected countries. Their responses – grounded in their knowledge of domestic legal systems, institutional structures, and practical enforcement realities – form the core of the country-specific sections that follow. As such, each country review reflects the experts' legal interpretation and insight into how relevant norms are applied in practice.

CROATIA

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER CROATIAN LAW,
AND NO CONFIRMED CASES OF
SPYWARE USE HAVE BEEN REPORTED.



The right to privacy in Croatia is constitutionally enshrined and broadly protected through a combination of national, EU, and international legal instruments. Article 35 of the Constitution¹⁰⁶ guarantees the respect and legal protection of private and family life, as well as personal dignity and reputation. This is reinforced by additional constitutional safeguards, including the inviolability of the home (Article 34), the confidentiality of communications (Article 36), and the protection of personal data (Article 37). Together, these provisions form a comprehensive framework for safeguarding privacy in both physical and digital domains.

Constitutional guarantees in Croatia are not absolute and may be restricted under specific, legally defined conditions. Article 36 allows for the limitation of the right to confidential correspondence and other forms of communication when necessary to protect national security or to conduct criminal investigations and prosecutions. Any such restriction must be legally justified and proportionate to the aim pursued.

The right to personal data protection is explicitly recognized in Article 37 of the Constitution, which states that personal data may be collected and processed only with the individual's consent or under specific legal provisions. The article also prohibits the use of personal data for purposes beyond those for which it was originally collected. Croatia's data protection framework is closely aligned with EU law. The General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) are directly applicable and have been implemented through two key national laws: the Act on the Implementation of the GDPR¹⁰⁷ and the Act on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities.¹⁰⁸

Within this framework, data processing without consent is permitted when it meets specific legal

grounds, such as compliance with legal obligations, the protection of vital interests, the performance of a public task, or the legitimate interests of the data controller. Derogations from data subject rights are allowed under Article 23 of the GDPR but must be lawful, necessary, and proportionate in a democratic society. For example, Article 21 of Croatia's GDPR Implementation Act permits the processing of biometric data by public authorities under defined conditions, while Article 24(3) excludes the application of biometric data rules altogether in matters relating to defense, national security, or intelligence services.

Under Article 47 of the Implementation Act, public authorities in Croatia are exempt from administrative fines. While this limits their financial liability, the Croatian Data Protection Agency still holds the authority to conduct investigations and issue corrective orders. The principles of necessity and proportionality are firmly embedded in Croatian data protection practice, helping to ensure that data processing is confined to what is strictly required to achieve legitimate objectives.

The confidentiality of electronic communications is strongly protected under both constitutional and statutory law. Article 36 of the Constitution guarantees the freedom and privacy of correspondence and all other forms of communication, encompassing both traditional and digital formats. At the legislative level, Article 43 of the Electronic Communications Act¹⁰⁹ prohibits the unauthorized interception, monitoring, or storage of electronic communications and related traffic data, except where expressly permitted by law – for example, under Article 52 or other sector-specific legislation concerning criminal procedure or national security. In addition, Article 142 of the Criminal Code¹¹⁰ prohibits unauthorized interference with communications, including the opening or retention of another person's mail or email, with penalties of up to one year of imprisonment.

While Croatian law does not explicitly identify data stored on digital devices as a distinct category, such data is broadly protected under existing privacy and data protection legislation. Article 37 of the Constitution guarantees the secrecy of personal data, extending to information stored or processed on digital devices. The GDPR and its implementing laws in Croatia apply equally to data stored locally or on cloud-based platforms, ensuring that processing is lawful and transparent. Additional sector-specific protections are provided by the Electronic Communications Act and the Cybersecurity

Act¹¹¹, which address the security and integrity of digital information systems.

The Croatian Criminal Code prohibits a wide range of offenses involving malicious software, including spyware. These offenses are grouped under Chapter 25, which addresses criminal acts against computer systems, programs, and data. Article 272, for example, prohibits the manufacture, sale, possession, or distribution of tools or software intended for use in committing other computer-related offenses, such as unauthorized access (Article 266), data interference (Article 267), or unauthorized interception of data (Article 269). While spyware is not explicitly named, these provisions effectively prohibit its development and use by criminalizing the underlying technical functions it relies on.

Although spyware is not explicitly mentioned in the law, relevant provisions – such as Article 266 on unauthorized access and Article 269 on interception of non-public data transmissions – clearly encompass activities associated with its deployment. Criminal penalties vary depending on the severity of the offense and the nature of the target, with harsher sentences applied when attacks are directed at state institutions, international organizations, or public-interest entities.

Special investigative measures are governed by the Criminal Procedure Act¹¹², particularly Article 332 and related provisions in Chapter 12. These measures are strictly regulated and may be used only when an investigation cannot be conducted by other means or could be carried out only with disproportionate difficulty. They require a written, reasoned request from the State Attorney and an order issued by an investigating judge. The judge acts as a legal safeguard, ensuring that the measures are lawful, proportionate, and respectful of the rights of the accused.

In urgent cases where delay would compromise the investigation, the State Attorney may issue a temporary order valid for up to 24 hours. This order must be submitted to the investigating judge within eight hours, accompanied by a written justification. The judge then reviews the order and, if necessary, refers the matter to a court chamber for a decision. If the chamber rejects the measure, all data collected under the temporary order must be destroyed.

Article 332 sets out the list of permissible special investigative measures, including the interception of telecommunications and computer data,

covert surveillance, the use of undercover agents, and simulated transactions. These measures may be extended for up to six months, depending on the category of offense and subject to judicial approval. The offenses for which such measures may be applied are listed in Article 334 and include serious crimes such as terrorism, human trafficking, sexual abuse of minors, corruption, and cybercrime.

Although the use of spyware is neither explicitly authorized nor prohibited under Croatian law, it likely falls within the scope of existing investigative measures, particularly the interception of computer data or remote access to IT systems. While the Criminal Procedure Act does not mention spyware by name, a subordinate regulation – the Ordinance on the Method of Conducting Special Investigative Measures¹¹³ – allows for interception to be carried out using “appropriate software solutions and technical interfaces”. However, there is limited public information regarding how such measures are implemented in practice.

Croatia’s legal framework does not formally distinguish between privacy in digital and physical spaces. While the Electronic Communications Act protects the confidentiality of digital communications, and the Criminal Code outlaws the unauthorized interception of electronic mail, the Criminal Procedure Act regulates searches and surveillance without explicitly differentiating between digital and physical domains. This absence of a specific legal distinction does not imply a lack of protection for digital privacy; instead, such protections are provided through a combination of general privacy laws and sector-specific legislation.

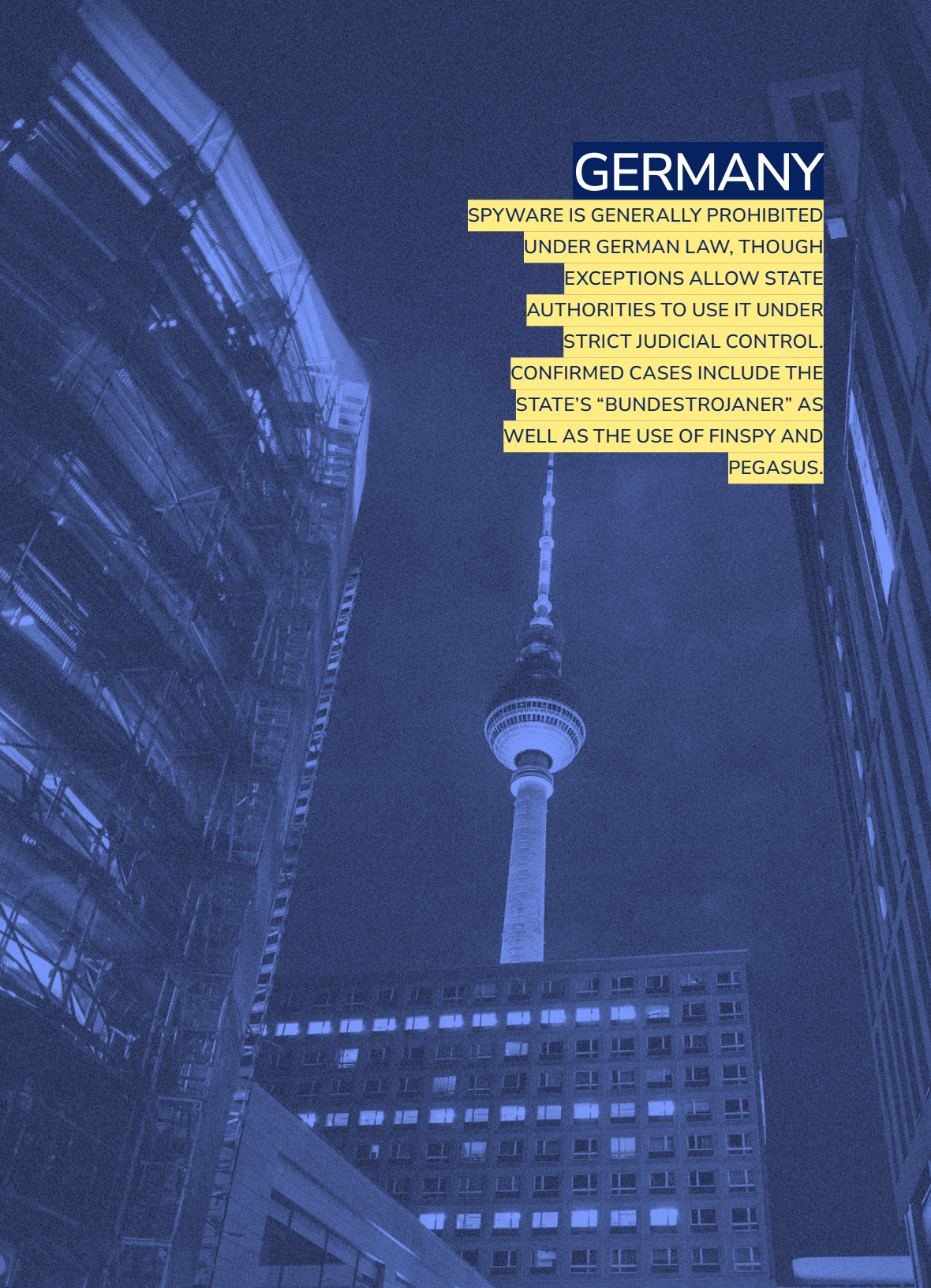
Finally, the unauthorized processing of personal data is a criminal offense under the Criminal Code. If such data is transferred abroad, made public, or used to obtain significant material gain or to cause substantial harm, the offense is punishable by up to three years of imprisonment. Surveillance of data stored on digital devices falls under the framework for special investigative measures outlined in the Criminal Procedure Act, ensuring that such activities are carried out only under strict judicial and legal oversight.

In conclusion, Croatia provides robust constitutional and statutory protections for privacy and personal data, reinforced by EU law. Although spyware is not explicitly regulated, the legal framework governing special investigative measures – along with the criminalization of core spyware functions – offers indirect limitations on its use. Nevertheless, the lack of

transparency in implementation and the absence of specific legal provisions contribute to ongoing uncertainty regarding the lawful deployment of highly intrusive surveillance technologies.

GERMANY

SPYWARE IS GENERALLY PROHIBITED UNDER GERMAN LAW, THOUGH EXCEPTIONS ALLOW STATE AUTHORITIES TO USE IT UNDER STRICT JUDICIAL CONTROL. CONFIRMED CASES INCLUDE THE STATE'S "BUNDESTROJANER" AS WELL AS THE USE OF FINSPY AND PEGASUS.



The German legal framework represents one of the most comprehensive and well-developed systems for safeguarding privacy and personal data in Europe, drawing from constitutional, civil, and criminal law. At its core is the German Basic Law (*Grundgesetz*)¹¹⁴, where the right to privacy is interpreted as an integral part of the broader right of personality. This right is rooted in Article 1(1), which guarantees the inviolability of human dignity, and Article 2(1), which protects personal freedoms and the free development of personality. The Federal Constitutional Court has further expanded these protections by recognizing the right to *informational self-determination* – granting individuals control over their personal data and autonomy in matters concerning their private lives. This protection explicitly extends to both physical and digital domains.

Article 10 of the Basic Law adds an additional layer of protection by affirming the inviolability of correspondence, post, and telecommunications, thereby securing the confidentiality of both traditional and electronic communications. This constitutional safeguard is further reinforced in civil law through Articles 823 and 1004 of the German Civil Code (*Bürgerliches Gesetzbuch*, BGB)¹¹⁵, which establish liability for violations of personality rights, including the unauthorized disclosure or use of personal information.

In the realm of criminal law, Division 15 of the German Criminal Code (*Strafgesetzbuch*, StGB)¹¹⁶ defines specific offenses related to the violation of private life. These include the unauthorized interception of conversations (Section 201), violations of intimate privacy (Section 201a), data espionage and phishing (Sections 202–202b), breach of private secrets (Section 203), and violations of postal or telecommunications secrecy (Section 206). Together, these provisions reflect the strong emphasis placed on protecting privacy and personal data at the national level.

Although privacy enjoys strong protection in Germany, the right is not absolute. Derogations are permitted under certain conditions, but only when grounded in statutory law and consistent with constitutional principles such as legality, legitimacy of purpose, and proportionality. Notably, however, human dignity – guaranteed under Article 1(1) of the Basic Law – is considered inviolable and cannot be restricted under any circumstances.

Personal data protection is governed by a multi-layered statutory regime. The Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG)¹¹⁷ complements the directly applicable EU General Data Protection Regulation (GDPR) and the Law Enforcement Directive. Articles 22 to 24 of the BDSG set out specific conditions under which personal data may be processed without consent – for example, in the public interest, for healthcare purposes, in criminal investigations, or in connection with legal claims. For public authorities, Article 3 BDSG permits processing when necessary to carry out official functions. Processing by private entities is also allowed under certain lawful conditions. In all cases, data processing must adhere to the constitutional principles of necessity and proportionality, as developed by the Federal Constitutional Court, to ensure the fundamental rights of individuals are not unduly infringed.

Special protections apply to electronic communications. Article 10(1) of the Basic Law guarantees the privacy of correspondence and telecommunications – a right further elaborated in the *Telecommunications-Telemedia Data Protection Act* (TTDSG).¹¹⁸ Section 3 of this law establishes telecommunications secrecy, covering both the content and metadata of communications, including failed connection attempts. Breaches of this secrecy are criminalized under Section 206 StGB, which provides for penalties of up to five years' imprisonment or fines for unauthorized disclosure by service providers or their employees.

Exceptions to these protections are allowed under Article 10(2) of the Basic Law, but only within narrowly defined legal frameworks. The G10 Act (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*)¹¹⁹ permits surveillance by federal intelligence services, including the BND, BfV, and MAD, for purposes related to national security and counterterrorism. Such surveillance must be approved by the G10 Commission, an independent oversight body, and is subject to strict limitations regarding scope, purpose,

and duration. Individuals are not notified of these measures, and any collected data must be treated confidentially.

Criminal investigations involving electronic communications are regulated by Sections 100a to 100g of the German Code of Criminal Procedure (*Strafprozessordnung*, StPO).¹²⁰ These provisions permit the interception of communications, remote access to IT systems, and other forms of surveillance, but only under conditions of judicial authorization and demonstrated necessity. Such measures are restricted to serious criminal offenses and must meet the standards of proportionality and necessity. In principle, individuals subject to surveillance must be informed once the measure has concluded, unless such notification would compromise the investigation.

A landmark development in German digital privacy law came with the Federal Constitutional Court's 2008 ruling in the "Online-Durchsuchung" case (BVerfGE 120, 274), which established a new fundamental right: the confidentiality and integrity of information technology systems. This right applies to digital devices as well as cloud-based systems and is derived from the inviolability of human dignity (Article 1(1)) combined with personal autonomy (Article 2(1)) of the Basic Law. It mandates that any state intrusion into IT systems must be based on a clear legal foundation, justified by exceptional threats – such as terrorism or imminent danger – and implemented using the least intrusive means available. Judicial authorization and procedural safeguards are required in all cases.

This jurisprudence had directly shaped the legal regulation of remote surveillance and spyware. Sections 100a and 100b of the StPO authorize covert remote access to digital devices and the surveillance of encrypted communications, often referred to as the use of "state trojans". These measures are restricted to serious criminal offenses and are subject to monthly judicial review, with any extended use requiring approval from the Higher Regional Court. The legal framework mandates precise identification of the target, a clear justification based on necessity and proportionality, and a detailed definition of the technical methods to be employed.

The use of spyware has been legally tested and remains highly controversial. The most prominent case – the "Bundestrojaner" scandal (2006–2008) – involved the Federal Criminal Police Office (BKA) deploying a surveillance trojan without a sufficient legal basis. In 2008, the Federal Constitutional Court ruled that such surveillance was unconstitutional in the absence of

specific legal authorization. In response, Germany amended laws such as StPO and the BKA Act to formally regulate the use of spyware, but civil society groups, including the Gesellschaft für Freiheitsrechte (GFF), have since challenged these amendments, arguing that they still do not meet constitutional requirements. One of these cases is currently pending before the Constitutional Court. Meanwhile, media investigations and a 2022 European Parliament study have revealed that German authorities have procured Pegasus spyware, raising further legal and ethical concerns.

Germany's approach to special investigative measures is also codified in procedural law. Sections 100a–100c of the StPO regulate various forms of surveillance, including:

- » Telecommunications interception;
- » Covert remote access to IT systems (*Online-Durchsuchung*);
- » Acoustic surveillance of private homes.

All of these measures require a court order, are subject to strict time limits, and must be justified based on necessity and proportionality. Procedural safeguards are detailed in Section 100e of the StPO, which mandates judicial authorization, a thorough statement of reasons, and prompt termination of surveillance once the legal conditions are no longer fulfilled.

Finally, the German legal system draws a clear distinction between privacy in physical and digital environments. Article 13 of the Basic Law guarantees the inviolability of the home, while Articles 1(1) and 2(1), as interpreted through case law, extend privacy rights to the digital realm. The Federal Constitutional Court has held that IT systems – because they store deeply personal data – deserve the same level of constitutional protection as one's home or personal correspondence.

Unauthorized access to IT systems, data espionage, and the use of surveillance software by private actors are criminalized under Sections 202 to 202c of the StGB. These provisions prohibit unauthorized access to data, interception of data transmissions, and the creation or distribution of hacking tools or malware, including spyware. Accordingly, while German law provides a narrowly defined legal basis for state use of spyware, it simultaneously prohibits its development, distribution, or use by unauthorized actors.

In conclusion, Germany has developed one of the most detailed and structured legal frameworks for regulating surveillance, data protection, and privacy across both physical and digital domains. While state use of spyware is formally authorized under strict conditions, its legal boundaries are narrowly defined and subject to judicial and civil oversight. Nevertheless, the continued deployment of invasive tools such as Pegasus, and the constitutional complaints still pending, highlight ongoing tensions between expanding state surveillance powers and the protection of fundamental rights in the digital age.

GREECE

SPYWARE IS PROHIBITED FOR PRIVATE ACTORS BUT MAY BE USED BY PUBLIC AUTHORITIES UNDER PENDING REGULATIONS THAT HAVE NOT YET BEEN ADOPTED. CONFIRMED CASES INCLUDE THE PREDATOR SPYWARE SCANDAL.



Privacy is a constitutionally protected value in Greece, and the confidentiality of communications holds a particularly prominent place within the legal system. Article 19 of the Constitution¹²¹ guarantees the secrecy of communications, allowing exceptions only under strictly regulated circumstances, such as threats to national security or investigations into serious criminal offenses. Any such exception must follow judicial procedures and are governed by a combination of constitutional safeguards and legislative provisions.

The primary laws regulating the lifting of communications secrecy are Law 3917/2011¹²² and Law 5002/2022.¹²³ Reflecting the now-repealed EU Data Retention Directive,¹²⁴ Law 3917/2011 regulates the retention and access to telecommunications metadata, including traffic and location data. Despite its outdated legal basis, the law remains in force and has been widely criticized by legal scholars and civil society organizations for failing to align with the standards set by the Court of Justice of the European Union (CJEU).

Law 5002/2022 represents a significant shift in the regulation of surveillance powers in Greece. Introduced in response to the 2022 wiretapping and spyware scandal, the law redefines the conditions under which communications confidentiality may be lifted. It authorizes surveillance in cases involving national defense, foreign policy, energy and cyber security, as well as a broad range of serious crimes, including corruption, organized crime, sexual offenses involving minors, and computer-related crimes. However, the law has raised serious concerns. Most notably, it transferred the authority to approve surveillance from an independent judicial framework to a mechanism that places greater control in the hands of the National Intelligence Service (EYP). Additionally, it removed the requirement for post-surveillance notification to individuals – a safeguard previously overseen by the

Authority for Communication Security and Privacy (ADAE) – thereby reducing transparency and limiting avenues for redress.

This shift has drawn criticism for undermining institutional checks and balances and weakening existing oversight mechanisms. The composition of the new supervisory body, which includes EYP officials and the president of ADAE, has been widely challenged for lacking the independence necessary to effectively safeguard fundamental rights.

Personal data protection is also enshrined in Article 9A of the Greek Constitution, which explicitly guarantees individuals protection against the unauthorized collection, processing, and use of their data, especially by electronic means. This constitutional right is further reinforced through the establishment of an independent supervisory authority, the Hellenic Data Protection Authority (DPA).

Greece's data protection regime is closely aligned with EU standards, incorporating the General Data Protection Regulation (GDPR)¹²⁵ and the Law Enforcement Directive (LED)¹²⁶, and implemented nationally through Law 4624/2019¹²⁷. This framework is further reinforced by sector-specific legislation covering areas such as electronic communications, banking secrecy, passenger data, and anti-money laundering. However, significant gaps remain, particularly in the area of national security. Article 10 of Law 4624/2019¹²⁸ exempts national security authorities from the supervisory oversight of the DPA, a provision that the authority itself has criticized as unconstitutional. This exemption has created a legal vacuum around some of the most intrusive forms of state data processing.

Surveillance systems such as Centaur and Hyperion, deployed by the Ministry of Migration and Asylum, have been challenged on these grounds. Legal advocacy groups, including Homo Digitalis, successfully petitioned the DPA to intervene, highlighting the ongoing tension between national security interests, and the legal and political controversy it continues to generate.

While constitutional and legal protections for communications and data are strong in principle, Greek law does not contain a dedicated provision specifically addressing the confidentiality of data stored on digital devices. Instead, protections in this area rely on general privacy, data protection, and criminal law provisions. Article 9 of the Constitution safeguards the inviolability of private life and the home, while Article 19 protects the

secrecy of communications in all forms, including digital. However, neither article expressly regulates local storage of data on devices like smartphones or computers.

With regard to the criminalization of unauthorized access to digital systems and spyware-related conduct, Article 370ST of the Penal Code¹²⁹, amended by Law 5002/2022, serves as the central provision. It prohibits the creation, distribution, possession, or use of software or devices capable of intercepting communications or extracting their content or associated metadata. The provision also penalizes the unauthorized handling of access credentials and information that could facilitate system breaches, particularly when used with criminal intent. The minimum penalty for such offenses is two years' imprisonment.

While this legislative reform addresses the private misuse of surveillance tools, it leaves open the possibility for their lawful use by public authorities, contingent on the adoption of a future Presidential Decree. As of April 2025, no such decree has been issued, and the specific conditions and safeguards governing the use of spyware by state actors remain undefined. This regulatory gap has fueled ongoing concern, particularly in light of past revelations regarding the use of surveillance technologies such as Predator in Greece. In the absence of clear legal standards, oversight mechanisms, and public transparency, civil society organizations and legal experts continue to warn of the risks posed by unchecked surveillance.

Special investigative measures – including covert data collection, surveillance, and communications interception – are regulated by Law 5002/2022.¹³⁰ Article 6 sets out the conditions under which the confidentiality of communications may be lifted for purposes of national security purposes or criminal investigations. Such measures require a reasoned request by a prosecutor and the approval of a judicial council, which must issue a decision within 48 hours. In exceptional circumstances, temporary authorization may be granted by a prosecutor or investigating judge, but it must be confirmed within three to five days to remain valid; otherwise, any evidence obtained is deemed inadmissible.

The law also introduces specific requirements for surveillance requests. Each request must include a description of the suspected offense, identification of the means of communication to be targeted, a justification grounded in necessity and proportionality, and details regarding the intended duration of the surveillance. Notably even third parties who are not suspected of any

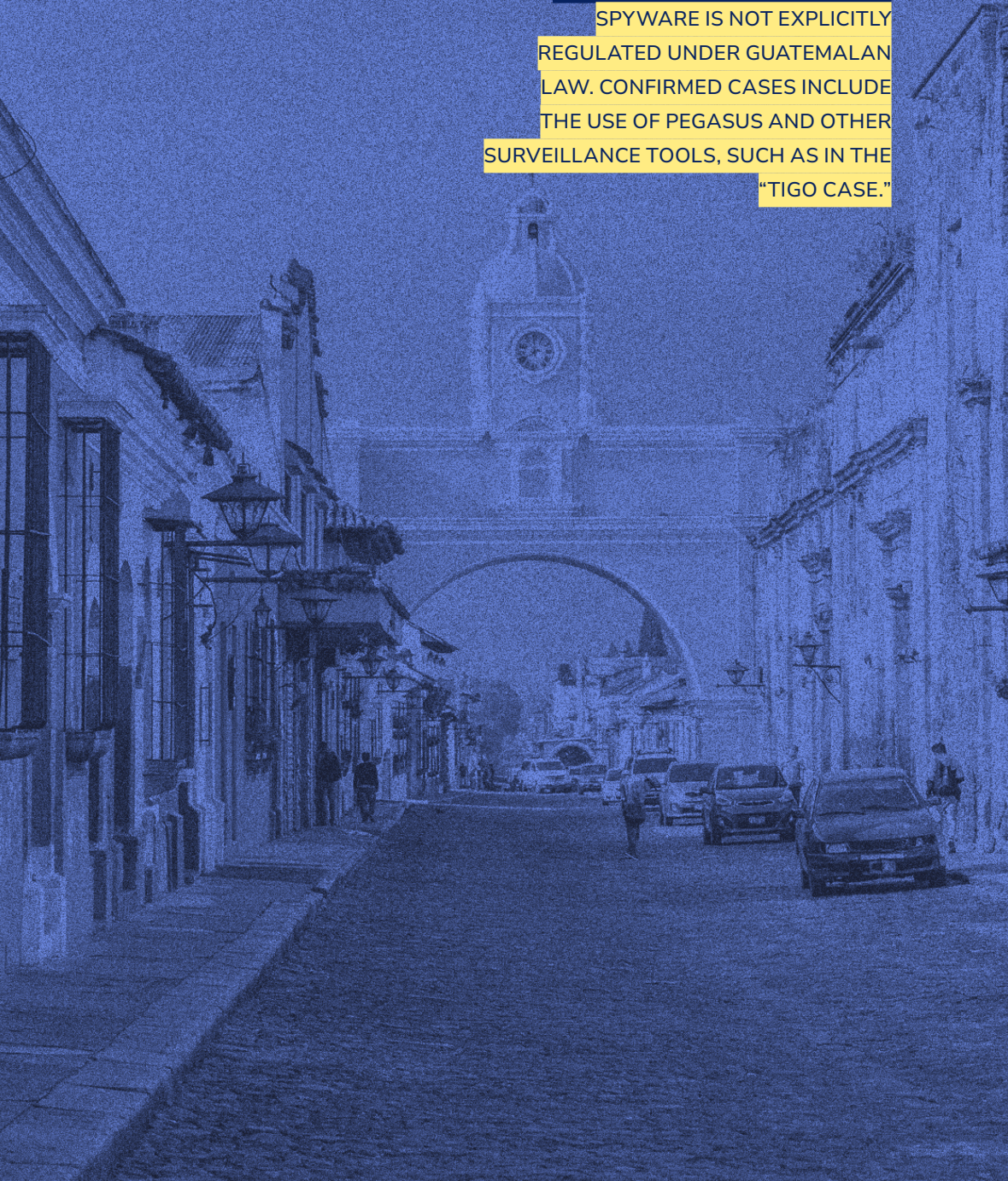
criminal activity may be subjected to surveillance if certain legal thresholds are met.

Article 5 of the same law governs the retention, processing, and destruction of data collected through surveillance. Unless justified by exceptional circumstances, such data must be destroyed within six months, and every action taken in relation to it must be properly documented. These provisions are intended to ensure traceability and to limit the risk of data misuse.

Overall, Greece's legal framework reflects a formal commitment to constitutional rights and alignment with EU law. However, in practice, enforcement and oversight mechanisms, particularly in relation to intelligence services and the use of spyware, remain underdeveloped. Recent legal reforms, introduced partly in response to public scandal, have raised as many questions as they have answered, especially concerning transparency, judicial independence, and institutional safeguards. Unless these issues are addressed with greater clarity and legislative precision, the tension between privacy and state surveillance in Greece is likely to persist.

GUATEMALA

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER GUATEMALAN
LAW. CONFIRMED CASES INCLUDE
THE USE OF PEGASUS AND OTHER
SURVEILLANCE TOOLS, SUCH AS IN THE
"TIGO CASE."



The right to privacy is constitutionally protected in Guatemala, through several provisions establishing foundational guarantees for personal and family life, the confidentiality of communications, and the inviolability of the home and correspondence. Articles 23, 24, and 25 of the Constitution¹³¹ explicitly shield individuals from unwarranted searches or intrusions into their homes, documents, and communications. The Constitutional Court has also played a key role in broadening the scope of these rights, notably recognizing the right to informational self-determination and privacy in its 2006 ruling (Exp. 1356-2006).¹³² These protections are not absolute, however. Under certain legal frameworks, particularly in organized crime investigations, exceptions are permitted with judicial authorization. For example, Decree 21-2002 (Organized Crime Law)¹³³ allows privacy rights to be limited when serious public crimes are suspected.

Guatemala does not have a comprehensive data protection law. Article 31 of the Constitution guarantees the protection of personal data, but this safeguard applies mainly to data held by public entities. The constitutional remedy of Habeas Data (Articles 30–35) grants individuals the right to access and correct public records. For data held by private entities, no dedicated regulatory framework exists, though the Constitutional Court has ruled that informed consent is required for private-sector data processing. Legal exceptions to consent are narrowly defined, such as under the Access to Public Information Law (Decree 57-2008)¹³⁴ or in criminal investigations governed by specific legislation, including the Law on Money Laundering and the Cybercrime Law (Decree 39-2022).¹³⁵

Some legal provisions, such as those in the Organized Crime Law, incorporate standards of proportionality, necessity, and temporality for state surveillance, particularly when personal data is involved. Government authorities may carry out surveillance and

data interception under several laws, including the Cybercrime Law and the Organized Crime Law, but only with judicial authorization. In practice, however, oversight is weak, implementation is inconsistent, and the scope of permissible surveillance remains broad.

The confidentiality of electronic communications is enshrined in Article 24 of the Constitution, which declares correspondence and communications inviolable. Any interception requires judicial authorization, as provided under Decree 21-2002. These protections apply to both traditional and electronic communications. Exceptions are permitted by law but must meet a high threshold of justification, such as addressing threats to public security or investigating serious criminal activity.

With respect to data stored on digital devices, Guatemala has no dedicated digital privacy law. Nonetheless, constitutional protections for documents and correspondence, together with provisions in the Criminal Code and Cybercrime Law, offer some safeguards against unauthorized access and data breaches. The Cybercrime Law (Decree 39-2022) proscribes identity theft, unauthorized access to computer systems, and data manipulation. While these provisions indirectly address surveillance of digital devices, there is still no comprehensive framework governing how either private or public sector may access such data.

In the area of cybercrime, the use of malware, viruses, and tools typically associated with spyware is proscribed under the Cybercrime Law. Although the term “spyware” is not explicitly used, the law prohibits unauthorized access to computer systems, illegal surveillance, and manipulation of digital information, core elements of spyware activity. Article 269 of the Criminal Code further outlaws the unauthorized interception and recording of data transmissions. These provisions apply both to private individuals and state actors, although enforcement in practice has proven challenging.

Despite these legal restrictions, Guatemala has been implicated in several high-profile cases of unlawful surveillance and spyware use by authorities. Civil society organizations such as Fundación Acceso and Citizen Lab have documented unauthorized monitoring with advanced tools, including Pegasus, ProxySG, Circles, and Pen-Link. Among the most prominent incidents was the “Tigo case”, involving high-level espionage carried out without judicial authorization and allegedly targeting political and business figures. The International Commission Against Impunity in Guatemala

(CICIG) investigated the matter, uncovering extensive abuse of surveillance capabilities by state actors.

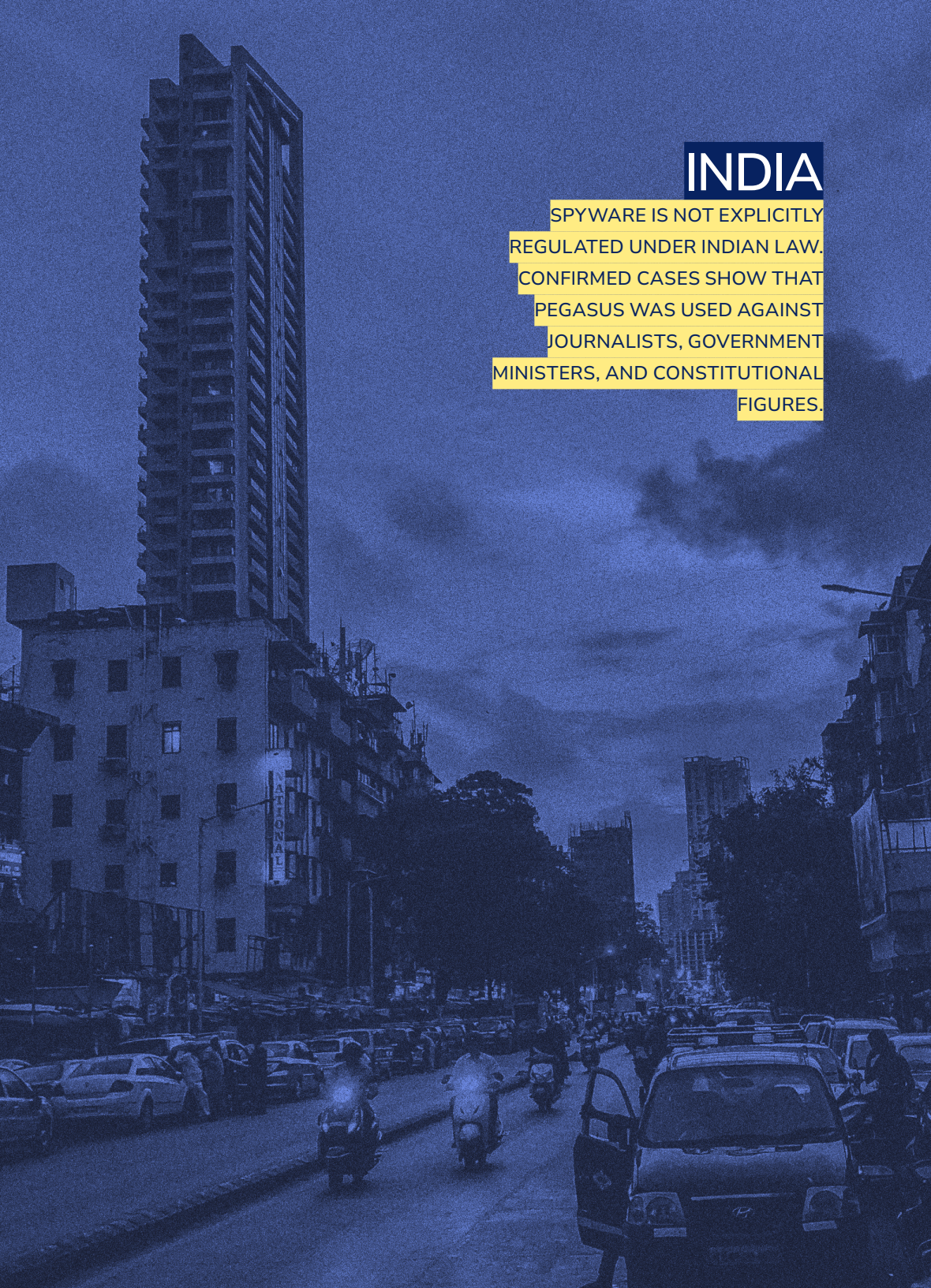
The legal basis for special investigative measures, including surveillance and data interception, is primarily set out in Decree 21-2002. Under this law, measures such as wiretapping or digital data collection must be requested by the Public Ministry and authorized by a judge. These investigative tools are permitted only when there is a well-founded suspicion of a serious crime and must comply with the principles of proportionality, temporality, and specificity. While the law does not explicitly address spyware, documented purchases and deployments by state institutions have created a legal grey area in which its use is neither clearly authorized nor expressly prohibited.

Guatemala's legal framework does not explicitly differentiate between privacy in digital and physical spaces. Instead, constitutional rights and criminal law combine to extend certain protections across both domains. The Cybercrime Law penalizes unauthorized access to systems, identity theft, and data manipulation, and requires judicial authorization for state surveillance of digital devices. However, the absence of a dedicated digital privacy law leads to inconsistent enforcement and limited transparency. Reports of extralegal surveillance underscore the risks posed by weak oversight and the potential misuse of technology for invasive monitoring.

In summary, while Guatemala's Constitution establishes core protections for privacy and data confidentiality, the overall legal framework remains fragmented and underdeveloped, especially in relation to digital privacy and surveillance technologies. The absence of a comprehensive data protection law and the ambiguous legal status of spyware create significant regulatory and accountability gaps. Although existing laws require judicial authorization for surveillance, these safeguards are often weakened by poor enforcement and the failure to address documented abuses. As a result, Guatemala's current legal environment continues to enable broad and potentially unlawful surveillance practices, raising serious concerns for the protection of fundamental rights in the digital era.

INDIA

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER INDIAN LAW.
CONFIRMED CASES SHOW THAT
PEGASUS WAS USED AGAINST
JOURNALISTS, GOVERNMENT
MINISTERS, AND CONSTITUTIONAL
FIGURES.



The right to privacy is constitutionally recognized as a fundamental right in India. However, this recognition has yet to materialize into a fully developed and consistently enforced data protection regime. The jurisprudential foundation for privacy protections rests on a three-part test articulated by Indian courts, which any state action infringing upon this right must satisfy. First, the action must have a basis in law – enacted by a competent legislature and compliant with constitutional provisions. Second, it must pursue a legitimate state aim, such as national security, crime prevention, or the delivery of welfare programs. Third, it must meet the test of proportionality, limiting interference with privacy strictly to what is necessary to achieve the stated objective.

India adopted the Digital Personal Data Protection Act (DPDPA)¹³⁶ in 2023, marking a significant step toward formalizing data protection framework. However, the law includes several broad exceptions that risk undermining its effectiveness, particularly in contexts involving state actors. Under the DPDPA, consent for data processing may be bypassed for vaguely defined “legitimate purposes” such as maintaining public order or for employment-related reasons. Moreover, data fiduciaries (entities corresponding to data controllers under GDPR) are not obligated to disclose essential information to data principals (data subjects), including third-party data sharing arrangements, data retention periods, or the specifics of cross-border data transfers.

More broadly, the Union Government (India’s central federal government) has the power to exempt certain categories of data fiduciaries, including government instrumentalities (i.e., state-controlled agencies or public bodies) and startups, from specific provisions of the law. These exemptions cover not only the processing conducted by the exempted entities themselves, but also any information they share with other state institutions. As a result, significant portions of state-led

data collection and processing may fall outside the core safeguards of the DPDP Act.

When it comes to proportionality, the Supreme Court's jurisprudence requires that any state derogation from the right to privacy must be proportionate to the legitimate aim pursued. In other words, the interference must be limited to what is strictly necessary to achieve the intended objective.

The Union Government has the authority to exempt any government instrumentality (GI) from the application of the DPDP Act. This exemption may also extend to any data processing carried out by the Union Government based on information received from an exempted GI. As a result, data collected by these instrumentalities would itself fall outside the scope of the law.

India's legal framework does not explicitly guarantee the confidentiality of electronic communications. Instead, interception is primarily governed by two statutes: the Indian Telegraph Act of 1885¹³⁷ and the Information Technology Act of 2000.¹³⁸ The Telegraph Act permits interception only in cases of public emergency or for public safety, and solely on specified grounds such as national security or the prevention of crime. In contrast, the IT Act – particularly following the 2008 amendments – significantly broadened the government's surveillance powers. It extended interception authority to all forms of digital communication and removed the prerequisite of emergency or public safety, thereby allowing interception in the context of any criminal investigation.

Furthermore, laws governing metadata retention and access impose significantly fewer restrictions than those for content interception. For example, under the Code of Criminal Procedure,¹³⁹ authorities generally do not need a court order to obtain metadata unless the service provider is categorized as a "postal or telegraph authority", a designation that does not extend to digital platforms such as email or social media providers.

India has no explicit constitutional or legislative provision guaranteeing confidentiality of data stored on digital devices. Although the right against self-incrimination is recognized in principle, it has not been consistently upheld in practice – particularly in situations where individuals are compelled to unlock or grant access to personal devices. The legal basis for digital surveillance primarily derives from Section 5(2) of the Telegraph Act and Section 69 of the Information Technology Act. These provisions

authorize the interception, monitoring, and decryption of digital information by the state, especially on grounds of national security or law enforcement. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules of 2009 further regulate the procedural aspects of such surveillance.

The legal regime addresses certain forms of digital intrusion, though not specifically spyware. Section 66 of the IT Act criminalizes unauthorized access to computer systems and malicious conduct such as data copying or dissemination of viruses, as detailed in Section 43. However, these provisions neither explicitly nor implicitly prohibit the development, distribution, or use of spyware, particularly when conducted by state authorities. India's criminal law contains no express provisions banning spyware or regulating its use in investigations. As a result, the deployment of such technologies exists in a legal grey zone.

India's approach to special investigative measures further underscores this legal ambiguity. Electronic surveillance is authorized under Section 69 of the IT Act, which permits the interception and decryption of digital communications. The procedural framework is set out in the 2009 Rules; however, oversight and transparency remain limited. Although the Telegraph Act prescribes a more restrictive standard – allowing interception only during public emergencies or for public safety – this safeguard has been effectively circumvented by the broader and more permissive regime established under the IT Act.

Legal access to metadata, in particular, remains subject to significantly less oversight. Since metadata is not uniformly protected under Indian law, law enforcement agencies often obtain such information without judicial authorization. This lack of scrutiny is especially concerning given the broad surveillance powers available to authorities and the absence of comprehensive legal safeguards to prevent abuse.

While the Indian Supreme Court has interpreted the right to privacy as encompassing both physical and informational domains, this constitutional interpretation has not translated into consistent or enforceable legal protections for digital privacy. Surveillance tools, including spyware, remain in a legal grey area – neither explicitly authorized nor clearly prohibited. As a result, constitutional guarantees coexist with broad discretionary powers, especially in matters of national security or public order, creating a

permissive environment in which surveillance technologies may be deployed without clear legal constraints or effective accountability mechanisms.

In sum, India's legal and institutional structure lacks strong, specific prohibitions on the use of spyware and does not offer a sufficiently robust regulatory environment to ensure proportionality, oversight, and transparency in state surveillance practices. As a result, while the right to privacy exists in theory, its effective protection remains uncertain in the face of expanding surveillance powers and rapidly evolving technologies.

INDONESIA

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER INDONESIAN LAW.
PUBLICLY KNOWN CASES INDICATE THE
USE OF PEGASUS SINCE 2018 BY POLICE
AND INTELLIGENCE SERVICES.

The right to privacy in Indonesia is formally recognized within the broader framework of constitutional and human rights protections. Article 28G(1) of the 1945 Constitution¹⁴⁰ guarantees every individual's right to personal protection, including their person, family, honor, dignity, and property, as well as the right to feel secure from threats or coercion in exercising their rights. These protections are echoed and elaborated in the Human Rights Law (Law No. 39/1999).¹⁴¹ Article 29(1) affirms the individual's right to protect their private and family life, reputation, and property, while Article 32 underscores the confidentiality of communication, both physical and electronic, stipulating that any interference must be authorized by a court order or its legal equivalent.

The protection of personal data was only recently consolidated under Law No. 27 of 2022 on Personal Data Protection (PDP Law),¹⁴² which establishes a comprehensive framework for data processing across both public and private sectors. The law grants data subjects key rights – including access, rectification, erasure, and the right to object or withdraw consent – and imposes obligations on data controllers to ensure transparency, security, and proportionality. However, despite this promising framework, the law contains broad exceptions. Article 17 permits derogations in areas such as law enforcement, national security, and financial supervision. These carve-outs allow state institutions to bypass core data protections guarantees without clear procedural safeguards or independent oversight.

Data processing without consent is also permitted under certain conditions, such as personal or household use, provided the data is not disclosed externally. While seemingly narrow, this exception leaves room for unregulated domestic data use. Moreover, enforcement of the regulation remains limited, particularly in the context of micro, small, and medium enterprise (MSMEs), where compliance is often hindered by the

complexity of technical requirements relative to their operational capacity. As of January 2025, the government recorded 64.2 million MSMEs in Indonesia, contributing over 60% of the country's GDP. This means a substantial share of financial and commercial activity takes place within a sector that operates with minimal regulatory oversight.

The law incorporates key data governance principles such as legality, proportionality, and the public interest. However, these standards are articulated in broad and abstract terms, without detailed guidance on their interpretation or practical application. As a result, while the principles offer theoretical safeguards, they have limited impact on regulating day-to-day data processing or state surveillance practices.

The confidentiality of electronic communications is primarily governed by the Telecommunications Law (Law No. 36/1999), which prohibits the unauthorized interception of communications transmitted over telecommunications networks. While this establishes a formal legal boundary against surveillance, the law remains vague regarding specific conditions under which state interception may be permitted. Further complicating the framework, Regulation of the Minister of Communication and Informatics No. 5 of 2020¹⁴³ requires private electronic system operators wishing to operate in Indonesia to provide government authorities with unfettered access to their services, including information regarding user personal data upon request by the government. This regulation had been widely criticized¹⁴⁴ by both domestic and international civil society organizations for lacking independent oversight, clear procedural safeguards, and protections against abuse.

Protections for the confidentiality of data stored on digital devices in Indonesia remain fragmented. The Law on Electronic Information and Transactions (EIT Law, as amended by Law No. 19/2016 and Law No. 1/2024) prohibits the unauthorized interception or redirection of electronic information (Article 31), while Article 258 of the 2023 Penal Code¹⁴⁵ criminalizes unlawful access to or interference with data stored on another person's devices. While these provisions aim to address hacking and data manipulation, they do not clearly differentiate between personal and institutional data, nor do they provide targeted safeguards or remedies for breaches involving sensitive or private information.

Despite the existence of relevant legal instruments, data breaches remain frequent in Indonesia, and institutional responses have been inadequate.

The country has experienced several large-scale breaches across different levels of governance, including a three-day shutdown¹⁴⁶ of the National Data Center due to a ransomware attack and a nationwide leak of healthcare data managed by Indonesian Social Security Agency. Notably, no official investigations or legal proceedings have been initiated in response to these incidents.

Indonesia's legal framework on spyware remains underdeveloped. The use of malicious software is addressed only indirectly through Article 33 of the EIT Law, which criminalizes actions that cause disruption or failure of electronic systems. However, this provision does not clearly extend to covert data collection, surveillance, or unauthorized data extraction, the core functionalities of spyware. There are no criminal law provisions that explicitly prohibit the development, possession, distribution, or use of spyware, whether by private individuals or state actors. This legal silence creates a regulatory vacuum, rendering the boundaries of surveillance technology ambiguous and largely unenforced.

Special investigative measures such as wiretapping or covert surveillance vary depending on the institution involved. For the National Police, these powers are regulated under the Law on the National Police (Law No. 36/1999). Article 32 permits surveillance based on a written order from a judge or an authorized official; however, it does not clearly define what constitutes sufficient grounds or outline the necessary procedural safeguards. This lack of specificity renders the framework vague and vulnerable to misuse.

In contrast, the Corruption Eradication Commission (KPK) operates under stricter conditions set out in Law No. 19/2019. The KPK may conduct surveillance, including communication interception and bugging, only after exhausting other investigative options and obtaining written approval from the Supervisory Board. The authorization is valid for up to six months and may be extended once. Data that is not relevant to the case must be promptly deleted. These provisions are more detailed and reflect a clear attempt to balance investigative needs with personal rights, though they apply only to a narrow set of cases.

The Police's internal Wiretapping Regulation requires the Chief of Police to authorize surveillance activities, which are carried out through telecommunications providers and limited to 30 days per approval. However, there is little public transparency regarding the use of these powers, and it remains unclear whether effective accountability mechanisms are in place.

The division between privacy in physical and digital spaces is not explicitly articulated in Indonesian law, but can be inferred from the gradual evolution of the legal framework. While older instruments such as the Human Rights Law focus on traditional protections of property and correspondence, newer legislation has addressed digital threats like unauthorized access, interception, and hacking. Nonetheless, Indonesia still lacks a unified conceptual and legal framework for digital privacy, particularly in relation to intrusive surveillance tools.

This gap is evident in the newly enacted Penal Code (Law No. 1/2023), where Article 333 criminalizes unauthorized access to and damage of protected state or public systems. The provision focuses on harm to the systems themselves rather than on violations of individual privacy. Notably, there is no corresponding article addressing covert surveillance or data extraction, underscoring the disconnect between data protection aspirations and criminal law enforcement.

Despite the increasing use of digital surveillance technologies, particularly against civil society actors, the state has yet to establish a clear legal framework. Incidents such as the 2020 breach of WhatsApp accounts during nationwide protests against military legislation – targeting activists, students, and journalists – remain unresolved and uninvestigated. In the absence of independent oversight or effective legal remedies, such incidents reinforce concerns over the unchecked deployment of digital surveillance without regulatory safeguards.

IRELAND

SPYWARE IS NOT EXPLICITLY

REGULATED UNDER IRISH LAW.


THERE ARE REPORTS THAT IRISH LAW

ENFORCEMENT HAVE MADE PAYMENTS

TO COGNYTE, AN ISRAELI SPYWARE

VENDOR.



A person wearing a dark jacket and carrying a white bag is walking away from the camera on a cobblestone street. To the left is a multi-story building with a sign that reads 'PRIVATE HOME' above a doorway. The scene is in black and white.

While the Constitution of Ireland¹⁴⁷ does not explicitly enshrine a right to privacy, Irish courts have long recognized privacy as an unenumerated constitutional right. This recognition stems from Article 40.3.1, which commits the State to “respect, and as far as practicable, by its laws to defend and vindicate the personal rights of the citizen”. Landmark cases such as *McGee v. Attorney General* (1974), which affirmed marital privacy, and *Kennedy v. Ireland* (1987), which extended privacy rights to communications, have solidified privacy as a fundamental right under Irish law. Additional constitutional protections for privacy also arise from provisions safeguarding private property, family life, the inviolability of the dwelling, and personal autonomy.

Beyond the national framework, Ireland is also bound by Article 8 of the European Convention on Human Rights (ECHR)¹⁴⁸, incorporated into domestic law through the European Convention on Human Rights Act 2003¹⁴⁹, and by Article 7 of the EU Charter of Fundamental Rights.¹⁵⁰ Both instruments protect private and family life, home, and communications from arbitrary interference. However, as clarified by Irish courts, including in *Kennedy v. Ireland*, these rights are not absolute and may be restricted in the public interest. Any restriction must be carefully balanced against competing rights and justified in accordance with constitutional and international standards.

Ireland’s legal framework for personal data protection is primarily shaped by EU law, particularly the General Data Protection Regulation (GDPR)¹⁵¹ and the Law Enforcement Directive (LED).¹⁵² Both have been transposed into national law through the Data Protection Act 2018.¹⁵³ The GDPR establishes six legal bases for processing personal data, with consent being one of them. It permits data processing without individual consent when it is necessary to comply with legal obligations, serve the public interest, or exercise official authority.

For law enforcement purposes, Part 5 of the 2018 Act gives effect to the LED, allowing competent authorities to process personal data for the prevention, investigation, or prosecution of crimes. The legislation permits derogations from individual rights, such as the rights to access or erasure, when necessary to prevent interference with legal proceedings or to protect national security. Sections 71 and 41 of the Act explicitly allow data to be processed and even repurposed when necessary and proportionate for purposes such as public safety and criminal justice. While this framework provides a comprehensive structure for lawful data processing, it also grants the state significant access to personal data under broadly defined conditions.

Oversight of this regime is entrusted to the Data Protection Commission (DPC), an independent authority responsible for monitoring compliance and enforcing data protection law. In practice, the DPC plays a central role in assessing the necessity and proportionality of personal data processing by both public and private entities.

The confidentiality of electronic communications in Ireland is primarily protected under the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011¹⁵⁴, which implement the EU's ePrivacy Directive. These rules prohibit the interception or access to electronic communications data without the user's consent or a specific legal basis. Despite these safeguards, Ireland maintains a data retention regime that permits state access to telecommunications metadata. The Communications (Retention of Data) (Amendment) Act 2022¹⁵⁵ governs the collection and disclosure of metadata, including call records and location data, by service providers. Under this law, such data may be retained and accessed without individualized suspicion, provided the request relates to serious criminal investigations, public safety, or national security. The Act also allows for real-time access to location data under defined conditions.

While these measures are intended to serve public safety objectives, the retention and access to metadata without individual suspicion continue to raise concerns about proportionality and oversight. Ireland's courts and institutions have yet to fully address the implications of these broad powers in light of evolving EU data protection standards and the jurisprudence of the Court of Justice of the European Union (CJEU).

Notably, Irish law does not contain specific provisions protecting the confidentiality of data stored on digital devices. Instead, protections in

this area are derived from general data protection laws and developments in case law. A significant milestone came with the Irish Supreme Court's ruling in *DPP v. Quirke* (2023), which recognized that digital devices serve as gateways to expansive virtual spaces containing highly sensitive and private information. The Court emphasized that search warrants targeting digital devices must explicitly specify that virtual content is being sought, acknowledging that digital privacy warrants a qualitatively different level of legal protection compared to traditional physical searches.

From a criminal law perspective, unauthorized access to digital systems is criminalized under the Criminal Justice (Offences Relating to Information Systems) Act 2017¹⁵⁶, which implements provisions of the EU Cybercrime Directive. This law prohibits the intentional introduction of malicious software, such as viruses or ransomware, and penalizes other forms of intrusion, including unauthorized access and denial-of-service attacks. However, Irish legislation does not contain any explicit provision criminalizing or regulating the creation, distribution, or deployment of spyware.

Although the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993¹⁵⁷ and the Criminal Justice (Surveillance) Act 2009¹⁵⁸ provide the main legal framework for targeted surveillance in Ireland, neither statute authorizes the use of spyware, understood as covert tools that provide full access to digital devices. Irish authorities have consistently declined to confirm or deny the use of such tools, pointing instead to these general statutory powers. The absence of express legal authorization or prohibition creates a legal vacuum, leaving the question of state use of spyware unresolved.

Special investigative measures in Ireland are governed by several laws. The 1993 Interception Act allows for the interception of communications, but unlike in most EU jurisdictions, it does not require judicial authorization; instead, approval is granted by the Minister for Justice. Similarly, access to retained metadata under the 2022 Amendment Act does not require judicial oversight and can be authorized internally by agencies such as the Garda Síochána or the Permanent Defence Forces. In contrast, the Criminal Justice (Surveillance) Act 2009 imposes more stringent safeguards for more invasive techniques, such as covert audio or video surveillance, which require judicial authorization under Section 7. However, tracking devices – for example, GPS units attached to vehicles – do not require judicial oversight

and may be approved internally by the investigating authority, as provided under Section 8 of the same Act.

This mixed regime of authorization standards – ministerial, judicial, and internal – creates inconsistency in the level of privacy protection across different surveillance techniques. Notably, Irish law contains no provision specifically authorizing the deployment of spyware or other highly intrusive digital surveillance tools, nor does it clearly prohibit their use.

In terms of how privacy is applied across physical and digital domains, Ireland is beginning to develop a more nuanced understanding of the differences between the two. The *DPP v. Quirke* judgment acknowledges the unique nature of digital spaces and the heightened privacy risks they present, particularly in light of the interconnectedness of devices, cloud storage, and third-party data. This evolving judicial perspective reflects a growing recognition of the need for distinct legal standards to govern digital surveillance.

In summary, Ireland’s constitutional and legal framework provides substantial – though not absolute – protection for privacy and data rights. These rights are reinforced by EU legislation and case law but are subject to broad exceptions, particularly in the areas of national security and law enforcement. The lack of explicit regulation or prohibition of spyware underscores a significant gap in Ireland’s legal architecture, raising critical concerns about transparency, proportionality, and oversight in the digital age.



ISRAEL

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER ISRAELI LAW,
THOUGH DRAFT LEGISLATION SEEKS
TO AUTHORIZE ITS USE BY POLICE.
CONFIRMED CASES INCLUDE THE USE
OF PEGASUS.

The right to privacy in Israel is enshrined in the Basic Law: Human Dignity and Liberty.¹⁵⁹ Article 7 guarantees each individual the right to privacy and intimacy, the inviolability of their private premises, and the confidentiality of conversations, writings, and personal records. These protections are reinforced by Article 8, which allows limitations only when enacted by law, serving a legitimate purpose and meeting the test of proportionality.

The Protection of Privacy Law (1981)¹⁶⁰ gives effect to constitutional privacy rights by defining violations and prescribing both civil and criminal penalties. It governs unauthorized surveillance as well as the collection and publication of personal data. However, Article 19 of the law explicitly exempts national security bodies – including the Israel Police, Internal Security Agency (Shin Bet), Foreign Intelligence Service (Mossad), and Military Intelligence – from liability, provided that infringements are “reasonably committed” in the course of official duties. This exemption substantially limits the reach of privacy safeguards in the context of state security operations.

Although Israel is not subject to the EU’s General Data Protection Regulation (GDPR),¹⁶¹ its data protection framework has been recognized as “adequate” by the European Commission.¹⁶² The Protection of Privacy Law permits data processing on lawful grounds such as consent, public interest, or legal obligation. However, the broad exemptions granted to security services significantly weaken the oversight mechanisms, particularly in matters related to national security.

A key legal instrument with significant implications for surveillance is the Wiretap Law (1979), which governs the interception of communications by state authorities. Although the law requires ministerial and judicial authorization for wiretapping, it contains

numerous exemptions and was not originally designed to address modern surveillance technologies such as spyware or remote access tools.

Another highly controversial legal instrument is the Criminal Procedure (Enforcement Authorities – Communication Data) Law, 2008,¹⁶³ commonly known in public discourse as the “Big Brother Law”. It grants law enforcement the power to collect communication metadata, including mobile phone location data, call logs, and ISP connection records, without prior judicial approval in many cases. Although presented as a crime prevention tool, the law has drawn sharp criticism from civil society groups and legal scholars for undermining privacy protections and enabling expansive state surveillance with minimal oversight. Critics argue that its broad scope, lack of transparency, and weak accountability mechanisms violate constitutional principles of privacy and proportionality. As such, the law has become a focal point in ongoing debates about surveillance powers in Israel.

In November 2024, the Israeli parliament (Knesset) gave preliminary approval to the so-called Spyware Law which seeks to formally authorize certain uses of spyware by the police for investigating serious crimes. While the bill includes safeguards such as court approval and explicitly excludes offenses related to political corruption, it has drawn strong criticism. Opponents, including the Attorney General, the Public Defender’s Office, and major human rights organizations, warn that the proposed law could be misused to target protesters or suppress political dissent. Particular concern centers on Section 157 of the Penal Code, which criminalizes rioting. Critics warn of the risk of abuse under the broad authority of the far-right Minister of National Security, Itamar Ben-Gvir, accused of politicizing law enforcement and eroding judicial oversight.

Existing investigative powers in Israel are already extensive. Special investigative measures – such as wiretapping, physical surveillance, and access to digital devices – are regulated under the Wiretap Law and the Criminal Procedure (Investigation Powers) Law. While these measures generally require court authorization, exceptions are permitted in cases involving imminent threats. Nevertheless, surveillance tools as invasive as spyware have outstripped the scope of existing legal definitions and procedural safeguards.

Furthermore, Israeli law does not formally distinguish between physical and digital privacy, although courts have increasingly acknowledged the

heightened sensitivity of digital data. For example, in a landmark decision issued by an expanded panel of nine justices, the Supreme court established detailed rules governing the procedures and judicial discretion involved in issuing search warrants for computers and mobile devices. The Court emphasized that the potential for privacy violations in such digital searches is infinitely greater than in “traditional” searches of an individual’s home or personal belongings.

The state’s increasing reliance on advanced surveillance technologies, such as Cellebrite tools, further complicates the legal landscape. These tools are employed not only by the police, but also by agencies such as the Tax Authority, the Privacy Protection Authority, and the Military Police.

In conclusion, while Israel provides strong formal guarantees for privacy through the Basic Law and statutory frameworks, these protections are often undermined by national security justifications, broad exemptions granted to intelligence services, and outdated legislation. The absence of a specific legal framework regulating spyware, the proposed Spyware Law, and the continued enforcement of the “Big Brother Law” all pose serious risks to the right to privacy. Absent substantial legal reform, meaningful judicial oversight, and robust accountability mechanisms, Israel’s surveillance practices are likely to remain at odds with democratic principles and international human rights standards.



MEXICO

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER MEXICAN LAW.
CONFIRMED CASES INCLUDE THE USE
OF FINFISHER, GALILEO, PEGASUS, AND
REIGN BY STATE AUTHORITIES.

The right to privacy in Mexico is constitutionally protected and reinforced by international human rights treaties, which carry the same legal authority as the Constitution.¹⁶⁴ Article 16 of the Mexican Constitution provides that “no one shall be disturbed in their person, family, home, papers, or possessions” without a written order from a competent authority that clearly sets out the legal grounds for such action. This protection extends to communications, which are declared “inviolable”, and any interference requires judicial authorization in accordance with strict procedural requirements.

Despite this robust constitutional framework, Mexico’s legal and institutional structures allow for broad and often opaque exceptions to these protections, particularly in relation to surveillance and personal data collection. Such exceptions are embedded in a range of laws, including the National Code of Criminal Procedures,¹⁶⁵ the National Guard Act,¹⁶⁶ the National Security Act, and the Federal Telecommunications and Broadcasting Law.¹⁶⁷ While these frameworks formally require judicial oversight and adherence to necessity thresholds, in practice they frequently enable expansive surveillance powers with minimal safeguards.

One of the most controversial provisions is Article 190, section II of the Telecommunications Law, which requires telecommunications providers to indiscriminately retain users’ communications records for two years. This blanket retention mandate applies to all users, regardless of suspicion or involvement in any legal proceeding, raising serious concerns about proportionality and sound data governance.

In the criminal justice context, Article 291 of the National Code of Criminal Procedures authorizes the interception of private communications, access to stored data, and real-time geolocation for criminal investigations. Although judicial authorization is formally required, this safeguard can be circumvented

through an “urgent” mechanism that permits the Public Prosecutor to initiate surveillance and seek retroactive judicial approval. In practice, this mechanism is widely used, effectively serving as a de facto bypass of judicial scrutiny.

Similarly, the National Guard Act authorizes access to stored communications data and real-time geolocation for crime prevention purposes. While Article 100 requires “sufficient evidence” that certain crimes are being planned or committed, this evidentiary threshold is broadly framed and lacks precise definition. Further uncertainty stems from Article 9, section XXVI of the proposed reforms to the National Guard Law, which creates ambiguity as to whether the National Guard must obtain judicial authorization to access telecommunications data or conduct real-time device tracking.

Mexico also enshrines the right to personal data protection in Article 16 of the Constitution, granting individuals the right to access, rectify, cancel, and object to the processing of their data. However, a series of legal reforms enacted on March 20, 2025, have substantially weakened core safeguards. These amendments affect both the Federal Law for the Protection of Personal Data in Possession of Obligated Parties¹⁶⁸ and the Federal Law for the Protection of Personal Data in Possession of Private Parties.¹⁶⁹ Under the revised framework, public authorities may process personal data without consent in a wide range of circumstances – from statutory mandates and inter-agency information sharing to emergencies and public health uses. While Article 80 of the public-sector law formally requires that such processing meet standards of necessity and proportionality, in practice these principles are inconsistently applied and often overridden by permissive secondary regulations.

These developments extend beyond the public sector. In telecommunications and financial services, data collection is automatic and indiscriminate: users are not asked for consent, and their information is retained and made available to authorities without individualized suspicion or judicial approval. Legislative proposals currently before the Mexican Congress would further expand state access, including plans to interconnect public and private databases in real time, implement a mandatory biometric identity system, and create centralized national platforms capable of tracking and verifying identities instantly. Civil society groups warn that, if enacted, these measures would fundamentally transform Mexico’s surveillance landscape, leaving

individuals with minimal control over their personal data and subjecting them to pervasive, unaccountable monitoring by state institutions.

The use of intrusive surveillance tools, such as spyware, exists in a regulatory vacuum. Mexican criminal law contains no specific provisions prohibiting the creation, use, or distribution of such tools. Article 177 of the Federal Criminal Code¹⁷⁰ makes the unauthorized interception of private communications a criminal offense, prescribing penalties of six to twelve years of imprisonment and substantial fines. However, this provision addresses only the interception itself, without regulating the development, deployment, or possession of spyware. As a result, the law does not treat spyware as a distinct threat, despite mounting evidence of its use by state actors against journalists, human rights defenders, and even public officials.

This legal ambiguity is particularly troubling given well-documented abuses. Investigative journalism, including the *Ejército Espía* report, has exposed the Mexican Army's illegal use of spyware against a broad spectrum of individuals, without consequence or accountability.¹⁷¹ A pending legislative reform package now risks retroactively legitimizing these practices. Article 29, sections XXI to XXIII of the proposed amendments to the Organic Law of the General Public Administration¹⁷² would grant the Ministry of National Defense (SEDENA) formal authority to conduct intelligence operations, including data processing and surveillance, absent any institutional safeguards or judicial oversight. Rather than remedying past violations, these reforms would entrench impunity and further lower the threshold for future surveillance.

Mexico's approach to special investigative measures is shifting in ways that further erode existing safeguards. The National Guard Act already grants security forces broad investigative and preventive powers, including digital surveillance and monitoring of publicly accessible online sources, yet it contains no detailed procedures, independent oversight mechanisms, or proportionality tests. Proposed amendments to this law and related statutes – including the General Law of the National Public Security System and the Law of the National Public Security Investigation¹⁷³ and Intelligence System¹⁷⁴ – would expand state access to personal data by creating mandatory telecommunications registries and enabling real-time geolocation, without safeguards or clear definitions of the competent authorities.

The Mexican legal framework does not formally distinguish between physical and digital privacy. Article 291 of the National Code of Criminal

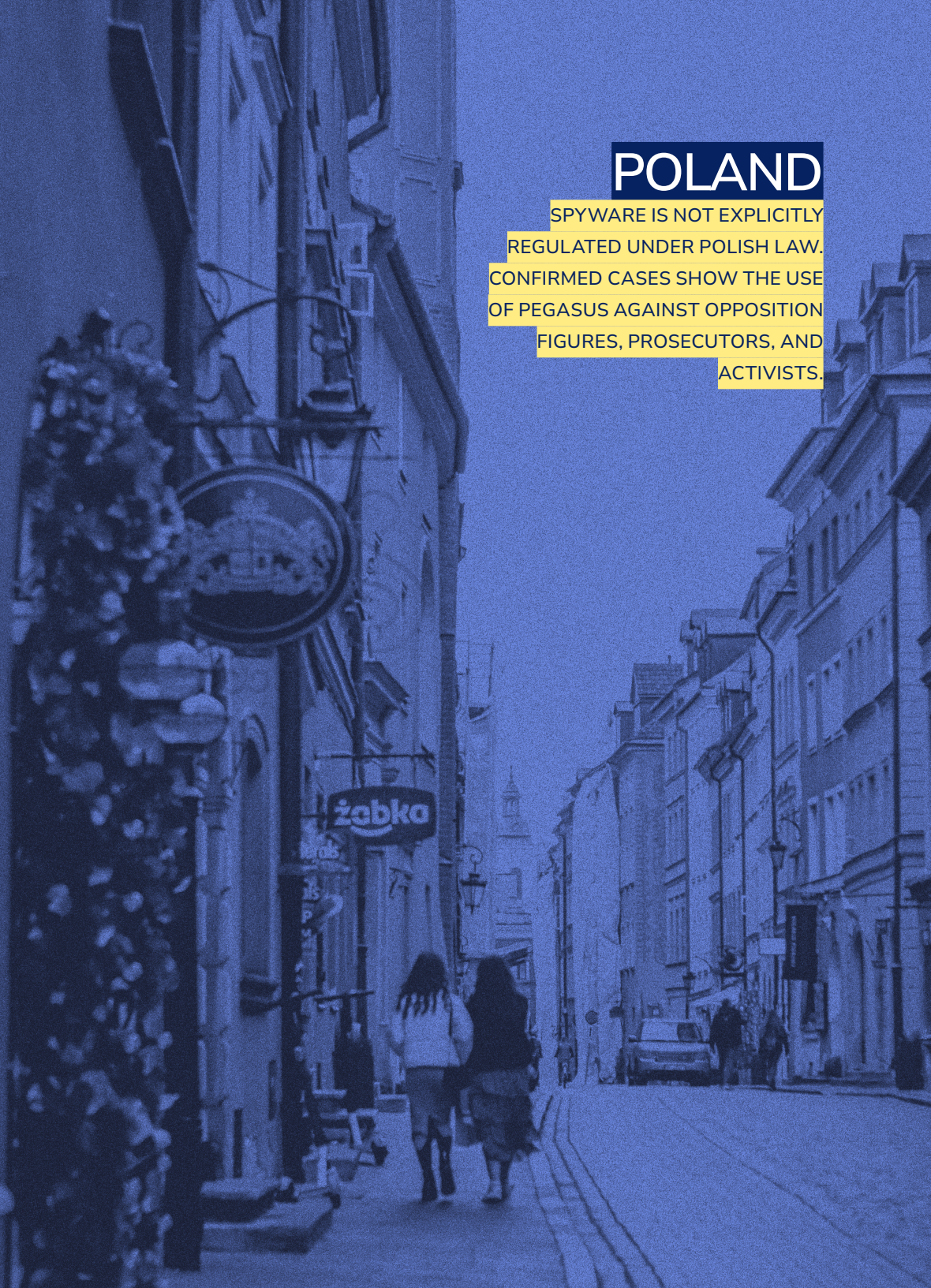
Procedure, as interpreted by the Supreme Court of Justice (SCJN), extends the protection of private communications to electronic and digital data. Under Article 16 of the Constitution, access to such data, including metadata and stored records, requires prior judicial authorization. In practice, however, protections are frequently undermined by vague mandates and broad interpretations by law enforcement, leaving uncertainty over which institutions are empowered to conduct surveillance and under what legal authority.

Although Article 177 of the Federal Criminal Code prohibits the interception of private communications without judicial authorization, it does not address the broader architecture of digital surveillance, which remains largely underregulated. The absence of targeted rules on spyware, combined with the widening gap between constitutional guarantees and everyday practice, leaves Mexico in a state of significant legal and institutional vulnerability.

In sum, while Mexico's Constitution and certain sectoral laws provide a strong formal foundation for privacy and data protection, practice tells a different story. Surveillance is often conducted without sufficient oversight or judicial authorization, recent reforms are eroding existing safeguards, and broad state access to data is becoming the norm. The lack of specific rules on spyware, combined with its documented misuse by state actors, poses serious risks to privacy and fundamental rights in Mexico's legal and institutional environment.

POLAND

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER POLISH LAW.
CONFIRMED CASES SHOW THE USE
OF PEGASUS AGAINST OPPOSITION
FIGURES, PROSECUTORS, AND
ACTIVISTS.



In Poland, the right to privacy is rooted in constitutional provisions and reinforced by both domestic and European legal instruments. Article 47 of the Polish Constitution¹⁷⁵ guarantees every individual the right to legal protection of their private and family life, honor and reputation, as well as the freedom to make decisions about their personal life. This is complemented by Article 51, which affirms the right to informational autonomy by prohibiting the collection, retention, or disclosure of personal data unless explicitly authorized by law. Together, these provisions lay a solid foundation for privacy protection in both physical and digital contexts.

Constitutional limitations on privacy rights in Poland are governed by Article 31(3), which permits restrictions only when established by statute and only if necessary in a democratic society to protect national security, public order, public health, morality, or the rights and freedoms of others. Any such restriction must respect the core essence of the affected rights and freedoms.

This constitutional framework is reinforced by the application of EU law, including the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), both of which have been incorporated into Poland's legal system. Polish data protection law recognizes multiple legal grounds for processing personal data – not only consent, but also public interest, legal obligation, protection of vital interests, and legitimate interests – provided the processing is proportional and necessary. However, these standards are not extensively defined in national legislation and are instead interpreted in light of EU case law, as well as decisions by the Polish Data Protection Authority and domestic courts.

In practice, the protection of personal data, particularly by state authorities, reveals several regulatory gaps. While the LED provides a general legal basis for

processing by competent authorities for criminal law purposes, oversight and transparency mechanisms remain weak, especially in relation to intelligence services. Institutions such as the Internal Security Agency, Military Counterintelligence Service, and Central Anti-Corruption Bureau are not subject to detailed sector-specific regulations on personal data. Moreover, they are often considered exempt from the scope of EU data protection law due to their national security functions. As a result, personal data processing in these sectors remains largely unregulated and opaque.

Communications privacy is further safeguarded by Article 49 of the Constitution, which guarantees the freedom and confidentiality of correspondence and other means of communication. This protection extends to digital communication channels such as email, messaging applications, and telecommunications, serving as a constitutional barrier against mass surveillance and arbitrary interception. However, the practical effectiveness of these protections is called into question when examining how surveillance is implemented in practice.

Under Article 19 of the Police Act¹⁷⁶, Polish law permits the interception of communications and the use of other special investigative measures, but only with prior court authorization and in cases involving serious crimes that cannot be effectively investigated by other means. These measures are subject to time limits, require a reasoned justification, and must follow formal procedures. In urgent situations, surveillance may begin without prior judicial approval but must be retroactively authorized by a court within five days. If such approval is not granted, the surveillance must be discontinued and any data collected must be destroyed.

However, concerns remain regarding the practical effectiveness of these safeguards. Judicial proceedings related to surveillance are conducted *ex parte*, involving only the requesting authority involved, and there is no obligation to notify individuals who were subjected to surveillance – even after the conclusion of investigations. Oversight mechanisms remain minimal. The Venice Commission has raised serious concerns about the adequacy of these protections, highlighting the absence of adversarial review, the limited role of the judiciary, and the lack of meaningful remedies available after surveillance has taken place.

The legality of highly intrusive surveillance technologies, such as spyware, is particularly problematic. There is no statutory provision in Polish law explicitly authorizing the use of tools like Pegasus. A detailed legal analysis

has found that such technologies violate multiple aspects of Polish law. Key concerns include the lack of authority to hack into end-user devices, the retrieval of data predating a surveillance order, the ability to alter device functions (such as remotely activating microphones or cameras), and the absence of system accreditation for handling classified information. Furthermore, the involvement of foreign entities – particularly the NSO Group, which developed Pegasus – raises additional concerns about data security and national sovereignty.

More broadly, Polish law does not draw a fundamental distinction between privacy in physical and digital spaces; the same constitutional principles apply to both. While this uniform approach offers a baseline level of protection, it also underscores the absence of a tailored legal framework to address the unique risks posed by advanced digital surveillance technologies. The regulation of data stored on or transmitted through digital devices is largely governed by general data protection law and the operational provisions of the Police Act, with no specific rules outlining how such surveillance should be conducted, limited, or overseen in the digital realm.

Unauthorized access to computer systems is criminalized under Article 267 of the Polish Criminal Code.¹⁷⁷ This provision penalizes unauthorized access to information systems, breaches of protective mechanisms, and the installation or use of surveillance devices. Sanctions include fines, restriction of liberty, or imprisonment for up to two years. While the law addresses both traditional and digital forms of privacy violation, its scope is limited and often requires a complaint from the affected individual to initiate proceedings.

In conclusion, while Poland has constitutional and statutory frameworks that protect privacy and personal data, the absence of explicit legal regulation for digital surveillance tools – coupled with weak oversight mechanisms – raises serious concerns. The use of spyware such as Pegasus illustrates how a lack of clear legal authorization and transparency can give rise to practices that potentially violate both domestic and international human rights standards.

An aerial, low-angle shot of a modern cable-stayed bridge at dusk. The bridge's tall, slender pylon and numerous stay cables are the central focus, extending from the bottom left towards the top center. The bridge deck curves into the distance. Below the bridge, a river or lake is visible with some boats and structures along the shore. The background shows a cityscape and distant hills under a dark, blue sky. The entire image has a monochromatic blue tint.

SERBIA

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER SERBIAN LAW.
CONFIRMED CASES INCLUDE ATTEMPTS
AT PEGASUS ATTACKS AND INFECTIONS
WITH A DOMESTIC TOOL KNOWN AS
NOVI SPY.

The right to privacy in Serbia is only partially guaranteed under the Constitution.¹⁷⁸ While the text does not explicitly recognize privacy as a standalone right, personal data protection is expressly guaranteed under Article 42, which serves as the primary constitutional safeguard in this area. This protection is further reinforced by Serbia's international human rights obligations, most notably the European Convention on Human Rights (ECHR), which is directly applicable within the domestic legal system.

Article 42 of the Constitution guarantees the protection of personal data and prohibits its use for purposes other than those for which it was originally collected, except in criminal proceedings or matters involving national security, and only when prescribed by law. It also grants individuals the right to be informed about data collected on them and to seek judicial protection against misuse. While the Constitution does not define privacy in broad terms, these provisions – especially when interpreted alongside Serbia's obligations under the ECHR – provide a partial foundation for safeguarding private life and informational autonomy.

Serbia's data protection regime is built around the domestic Personal Data Protection Act¹⁷⁹, which is largely aligned with the EU General Data Protection Regulation (GDPR) and the Police Directive (EU) 2016/680. This Act serves as the primary legal framework governing the collection, storage, processing, and sharing of personal data. It sets out the standard legal bases for data processing – consent, legal obligation, public interest, vital interest, and legitimate interest – and enshrines key principles such as data minimization, proportionality, and purpose limitation. Public authorities are permitted to process personal data without user consent, but only when explicitly authorized by law.

The collection of personal data by the police is regulated as an exception to the general data protection regime. Police authorities operate under conditions that largely reflect those set out in the Police Directive, meaning their obligations are generally less stringent than those applicable to other data controllers. Fewer legal requirements apply; however, certain conditions and obligations must still be met. Data processing must be legally authorized, a Data Impact Assessment Study (DIAS) must be prepared when required, and police authorities must adhere to core data protection principles, including transparency.

The confidentiality of electronic communications is protected under Article 41 of the Constitution, which guarantees the secrecy of letters and other forms of communication. This general constitutional safeguard is further elaborated in the Law on Electronic Communications¹⁸⁰, which requires service providers to maintain the confidentiality of user data and prohibits its disclosure without user consent, unless otherwise provided by law. Exceptions exist primarily for purposes of criminal investigation and national security, and require a valid legal basis, most often in the form of a court order.

There is no specific legislation in Serbia that separately regulates the confidentiality of data stored on digital devices. However, general constitutional protections and data protection laws apply. In addition, the Criminal Procedure Code¹⁸¹ provides heightened protection for devices used for automatic data processing, such as smartphones and computers, within the framework of search and seizure procedures. Unlike searches of homes or persons, which may be conducted without a warrant in narrowly defined and exceptional circumstances, searches of digital devices always require prior judicial authorization, without exception. Although not explicitly framed as a higher tier of protection, this legal distinction effectively affords digital devices stronger safeguards, reflecting the heightened sensitivity and volume of private information they contain.

Serbia's Criminal Code¹⁸² prohibits a broad range of cyber-related offenses, including unauthorized access to computer systems (Article 302), computer sabotage (Article 299), and the creation or distribution of malicious software (Article 300). Article 304a further prohibits the production or dissemination of tools intended for the commission of cyber offenses, encompassing functionalities typical of spyware. While the term “spyware” does not appear explicitly in the legislation, the activities commonly associated with it – such as unauthorized surveillance, keylogging, or data exfiltration – are addressed through broader criminal provisions.

However, Serbian criminal law does not explicitly prohibit or regulate the use of spyware by state authorities. There are no legal provisions that directly govern the deployment of intrusive surveillance software, whether for national security or law enforcement purposes. As a result, the use of spyware occupies a legal gray area – neither expressly authorized nor clearly restricted.

SECRET SURVEILLANCE OF COMMUNICATIONS	SPYWARE
It refers exclusively to communication - e.g. phone calls, text messages.	Provides full access to all content – gallery, documents, location, apps, etc.
The phone number is being monitored.	The entire device is monitored, including all data without limitation and selection (including the data of all third parties that have ever been in communication with the owner of the device)
Supervision is time-limited, determined by the court.	Spyware is always active.

SECRET OBSERVATION AND RECORDING	SPYWARE
It can be used to discover the suspect's contacts and communications.	Access all interactions, including private, business and non-relevant information.
It is allowed only in public places, places with limited access and premises, but not in the apartment.	Indiscriminate, active always and everywhere, even in the apartment.
There is control and the legal possibility of review	The surveillance is secret, without informing the victim and often beyond the control of the judiciary.

SPAIN

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER SPANISH LAW.
CONFIRMED CASES INCLUDE THE
USE OF PEGASUS AND CANDIRU,
PARTICULARLY TARGETING CATALAN
POLITICIANS, JOURNALISTS, AND CIVIL
SOCIETY MEMBERS.



The legal framework provides robust constitutional and legislative protections for privacy and personal data, aligning closely with European Union standards and jurisprudence. The cornerstone of these protections is Article 18 of the Spanish Constitution¹⁸³, which guarantees personal and family privacy, the inviolability of the home, and the secrecy of communications. These rights may only be limited through judicial authorization and are firmly rooted in the principles of legality, necessity, and proportionality.

Article 18.2 of the Constitution prohibits entry into a private residence without the occupant's consent or a judicial warrant, except in cases of *flagrante delicto*, when a crime is being actively committed. Similarly, Article 18.3 establishes that any interception of communications, including telephone and electronic correspondence, requires prior judicial authorization. In the context of criminal investigation, the Spanish Criminal Procedure Act¹⁸⁴ (*Ley de Enjuiciamiento Criminal*, LECRIM) provides further regulation, particularly following reforms introduced in 2015. These reforms codified the use of digital investigative tools, such as communication interception, remote access to IT systems, GPS tracking, and covert surveillance, under strict judicial oversight.

Constitutional protections in Spain extend into the digital domain through Article 18.4, which requires that the use of information technologies be limited by the law to safeguard citizens' honor and privacy, and guarantees the full exercise of their fundamental rights. This provision serves as the constitutional foundation for Spain's data protection regime, particularly in relation to new technologies.

As a member of the European Union, Spain is subject to the General Data Protection Regulation (GDPR)¹⁸⁵ and the Law Enforcement Directive (LED)¹⁸⁶, both of which have been transposed into national law. Organic Law 3/2018 on the Protection of Personal Data and

Guarantee of Digital Rights (LOPDGDD)¹⁸⁷ complements the GDPR and incorporates the Law Enforcement Directive. This legal framework applies to both the public and private sectors, defining the conditions under which personal data may be collected, processed, and stored. Law enforcement agencies are specifically governed by Organic Law 7/2021¹⁸⁸, which regulates data processing in the context of criminal investigations and ensures that such processing remains necessary, proportionate, and subject to accountability mechanisms.

The Criminal Procedure Act (*Ley de Enjuiciamiento Criminal*, LECRIM)¹⁸⁹ plays a central role in regulating special investigative measures. Articles 588 *bis* through 588 *octies* govern the use of techniques such as communication interception, GPS tracking, covert audio and video surveillance, and remote access to or manipulation of IT systems. These measures are permitted only when strictly necessary, when less intrusive alternatives are unavailable, and only with prior judicial authorization. Procedural safeguards ensure that each measure is proportionate to the seriousness of the offense under investigation and is strictly limited in both duration and scope.

While these legal provisions reflect a formal commitment to fundamental rights, their application in practice has raised serious concerns. Independent investigations and civil society organizations have documented abuses, particularly involving the use of spyware against political opponents and activists. One of the most prominent cases involved the deployment of Pegasus spyware against Catalan political figures. Although these actions were formally carried out under judicial procedures, they underscore the risks of overreach and the limitations of institutional safeguards in fully protecting individuals from intrusive surveillance technologies.

Spain's approach to confidentiality in electronic communications is similarly rigorous. Article 18.3 of the Constitution, together with sector-specific laws such as Law 9/2014 on Telecommunications¹⁹⁰ and Law 34/2002 on Information Society Services and E-Commerce (LSSI-CE)¹⁹¹, protects private communications from unauthorized access. These statutes require service providers to maintain the secrecy of communications and prohibit interception without user consent or prior judicial authorization. The GDPR and the transposed ePrivacy Directive (2002/58/EC) further strengthen this framework by establishing legal bases for independent oversight and embedding core principles such as data minimization.

Nevertheless, Spain lacks specific statutory provisions that directly address the confidentiality of data stored on digital devices. Instead, protections for such data are derived from broader legal standards related to data protection, the right to privacy, and the regulation of investigative measures under The Criminal Procedure Act (LECRIM). Unauthorized access to digital devices is criminalized under data protection laws and related criminal provisions, particularly when such access occurs without consent and outside the limits set by judicial authority.

There are likewise no explicit provisions in Spanish criminal law that address spyware as a distinct category of technology. While general criminal offenses, such as unauthorized interception of communications or illicit access to computer systems, can be applied in cases involving spyware, there is no legal definition or tailored regulation specifically targeting its development, distribution, or use. This regulatory gap means that while misuse of surveillance technologies may be prosecuted under existing legal categories, their deployment by state authorities remains subject only to general legal principles, rather than specific statutory prohibitions.

Spain's legal system draws a clear conceptual distinction between privacy in physical and digital spaces, while ensuring that both are constitutionally protected. Safeguards for physical spaces stem from Article 18.2 of the Constitution, whereas digital privacy protections are grounded in Article 18.4 and further developed through legislation such as the LOPDGDD and LECRIM. The Spanish Constitutional Court has affirmed that access to metadata and stored digital information constitutes an interference with the inviolability of private communications and must, therefore, be subject to judicial oversight.

In the context of criminal proceedings, the LECRIM regulates access to digital data through provisions that require judicial warrants and impose clear limitations. Remote access to IT systems, including digital searches and data collection from computers and mobile phones, is permitted only under the stringent conditions set out in Articles 588 *septies* (a-f). Such measures must meet the criteria of legality, necessity, and proportionality, and must be conducted under judicial supervision.

In conclusion, Spain upholds a privacy and data protection framework that is firmly rooted in constitutional principles and closely aligned with EU standards. The regulatory structure is well-developed and supported by judicial safeguards intended to constrain the use of invasive investigative

measures. However, the lack of spyware-specific legislation, along with documented instances of misuse in politically sensitive cases, indicates that existing protections – though robust in theory – may be susceptible to circumvention in practice. Ongoing oversight and institutional reform may be necessary to ensure that Spain’s commitment to privacy remains effective amid evolving technological and political challenges.

TURKEY

SPYWARE IS NOT EXPLICITLY
REGULATED UNDER TURKISH LAW.
CONFIRMED CASES INCLUDE THE
USE OF FINSPY DURING OPPOSITION
PROTESTS IN 2017.



The constitutional and legal framework in Turkey provides formal protections for privacy and personal data, but enforcement remains inconsistent and is frequently undermined by broad exceptions available to public authorities. Articles 20 and 22¹⁹² of the Constitution explicitly guarantee the right to private and family life, the protection of personal data, and the confidentiality of communication. These rights may be restricted only by judicial order and under narrowly defined grounds such as national security, public order, or crime prevention. In urgent cases, authorities may act with written authorization from a competent public body, subject to subsequent judicial review.

These constitutional guarantees are further reinforced by provisions in Turkish Criminal Code.¹⁹³ Article 134 criminalizes violations of private life; Article 135 prohibits the unlawful collection of personal data; and Articles 136 and 138 provide additional legal safeguards. The Turkish Civil Code¹⁹⁴ also recognizes general rights to privacy and human dignity. Nevertheless, legal scholars and civil society organizations have repeatedly expressed concern about the practical enforcement of these rights, especially in cases involving surveillance and the invocation of national security interests.

Turkey's Personal Data Protection Law,¹⁹⁵ enacted in 2016 and modelled on EU standards, establishes key individual rights, including access, rectification, and erasure of personal data. It requires that data processing be based on explicit consent or a clear legal basis, and mandates adherence to principles such as lawfulness, fairness, and purpose limitation. However, state institutions enjoy broad exemptions. The National Intelligence Organization (MIT), in particular, operates with expanded powers under national security and counterterrorism laws, which lack meaningful external oversight. The vague and expansive nature of these exemptions undermines legal safeguards and enables intrusive surveillance practices.

Reports by international organizations such as Privacy International and Citizen Lab indicate that Turkish authorities have procured – and potentially deployed – surveillance technologies and spyware, including systems developed by Gamma International (FinFisher), Hacking Team, and Blue Coat. These tools enable the remote extraction of communications, files, and metadata from personal devices – activities that raise serious legal and constitutional concerns, particularly given the absence of explicit statutory authorizations or effective procedural safeguards.

Turkish law contains no provisions that explicitly regulate the use of spyware. Nor are there statutes establishing a detailed framework for its deployment, oversight, or ex post accountability. At the same time, the Criminal Code neither explicitly nor implicitly prohibits spyware. While activities such as unauthorized interception of data, disruption of computer systems, and unlawful access to personal information are criminalized, these provisions do not clearly extend to the covert use of state-sponsored spyware. This legal silence, combined with the broad and largely unchecked powers of intelligence and law enforcement agencies, has created a regulatory vacuum in which spyware use is neither formally authorized nor meaningfully constrained.

Special investigative measures are formally regulated under the Turkey’s Criminal Procedure Code (Law No. 5271), which authorizes techniques such as wiretapping, the search and seizure of digital devices, and access to computer systems. These measures require a court order and are intended to be applied only in the investigation of serious crimes. In practice, however, judicial oversight is often limited. EU assessments and human rights reports have repeatedly raised concerns about insufficient legal safeguards, lack of transparency, and the limited independence of the judiciary.

A 2024 report by the European Commission¹⁹⁶ found that Turkey’s data protection regime and investigative practices remain misaligned with EU standards. For instance, while access to digital systems for investigative purposes is subject to formal authorization requirements, the legal thresholds of necessity and proportionality are vaguely defined and seldom enforced in practice.

Turkish law does not draw a legal distinction between physical and digital privacy, nor does it provide specific protections for data stored on personal devices such as smartphones or computers.

Furthermore, there is no dedicated legislation governing the confidentiality of electronic communications or the integrity of data stored on digital devices. In several areas – particularly in relation to the surveillance of activists, journalists, and opposition figures – the legal framework lacks the specificity, transparency, and judicial oversight needed to prevent abuse. Decisions concerning surveillance or access to personal data are frequently made within opaque bureaucratic structures, with minimal public oversight and few legal remedies available to those affected.

In this context, and in the absence of clear legal provisions either prohibiting or expressly authorizing the use of spyware, the legal status of such technologies in Turkey must be assessed indirectly. Given the weak enforcement of privacy safeguards, the broad discretionary powers afforded to state institutions, and the opacity of surveillance practices, there appears to be no effective legal barrier to the deployment of spyware by public authorities. On the contrary, the current legal and institutional landscape seems to enable such practices *de facto*, despite their formal lack of regulation.

CONCLUSION

This comparative legal analysis reveals an alarming pattern across all jurisdictions: the use of spyware remains largely unregulated, and in most cases operates in the legal shadows, tolerated through vague national security exceptions, outdated investigative powers, or tacit gaps in the law. While some countries provide stronger constitutional and statutory safeguards for data protection than others, none of the legal systems examined in this study have developed a coherent and transparent framework that respects rights while addressing such intrusive technologies as spyware.

However, the absence of explicit regulation should not be seen as a legislative omission awaiting correction. On the contrary, the invasive nature of spyware – its ability to access, monitor, and manipulate entire digital ecosystems – renders it incompatible with the core principles of human dignity, privacy, data protection, freedom of expression, as well as fundamental and long-standing guarantees such as the presumption of innocence. Spyware is not a tool that can be made acceptable through better laws; it is a technology whose use in democratic societies must be categorically rejected.

Attempts to integrate spyware into legal systems, often justified by crime prevention or national security, risk normalizing human rights violations at the highest level and under the cover of law. Even when subject to judicial oversight, the very logic of spyware undermines basic principles such as necessity, proportionality, and transparency. No warrant, no procedural safeguard, can justify the all-encompassing surveillance that spyware enables.

This study does not call for new regulatory frameworks that would ultimately legitimize spyware, but rather affirms the urgent need to resist its institutionalization. Democratic societies must draw a clear normative boundary: spyware, by its design, function, and effect, constitutes a violation of the rule of law. The way forward is not regulation, but prohibition.

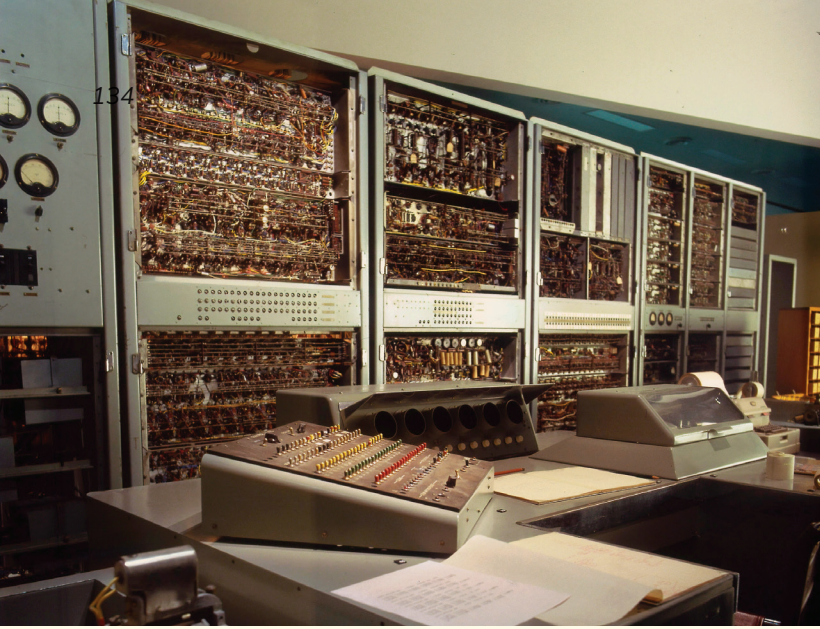
PRACTICE



PRACTICE

The capture of information and use of intrusive surveillance constitute the backbone of repressive and authoritarian regimes worldwide. Such surveillance can take many forms – ranging from physical tracking and monitoring to bugging private residences and workplaces, and remotely infiltrating digital devices. Among these, device infiltration has emerged as one of the most effective methods. It provides a direct and continuous link to the targeted individual, often without their knowledge, and is notoriously difficult to detect. As discussed in the previous chapter, this practice often exists in a legal gray zone. Its use is rarely explicitly authorized, but neither is it clearly prohibited – making prosecution, especially in cases involving state actors, exceedingly difficult.

In 2024, global internet freedoms declined for the 14th consecutive year, marking a sustained and troubling trend of increasing political pressures and persecution, both online and offline.¹⁹⁷ Digital tools have become central to state strategies for suppressing dissent and silencing critics. In many cases, human rights defenders, journalists, opposition figures, and members of civil society have been subjected to unlawful, targeted surveillance.¹⁹⁸ Depending on each state's technical and financial capacities, this has involved both commercial spyware acquired from private vendors and domestically developed surveillance tools. To understand how spyware has become embedded in contemporary surveillance practices, this chapter traces its emergence and use across several key trajectories: the erosion of human rights safeguards in state surveillance, the expansion of the spyware industry within complex geopolitical landscapes, and the normalization of invasive technologies in everyday life.



THE SOCIO-CULTURAL HISTORY OF SURVEILLANCE

The impulse of the state to monitor its citizens is not new. Before the rise of advanced technologies, surveillance relied largely on the physical presence and capacity of law enforcement to observe activity in public and private spaces. As technology evolved, modes of communication shifted – from face-to-face meetings, scheduled phone calls, and fax machines to smartphones and the instantaneous exchange of information online. States have generally adapted more effectively to earlier waves of technological change, as these tools were adopted gradually by the public. In contrast, the rapid and widespread uptake of newer-generation technologies has often outpaced regulatory and institutional responses.¹⁹⁹

In the 20th century, communication surveillance was relatively straightforward, owing to the centralized structure of telephone switchboards. Law enforcement agencies could intercept conversations simply by gaining physical access to these hubs, facing few technological obstacles. However, as communication technologies advanced, interception methods grew significantly more complex, requiring increasingly sophisticated tools and infrastructure.

Today most communications – including phone calls, messages, and internet data – are routed through the Global System for Mobile

Communications (GSM), generating metadata that can be readily accessed by law enforcement and security agencies via mobile network operators, typically with a valid court order. Interception of the content itself is carried out through wiretapping, which involves listening to and recording live phone calls to gather intelligence on people of interest. However, historical patterns reveal a consistent tendency among law enforcement and security agencies to overreach, extending wiretapping practices to monitor political opponents, members of civil society, and even geopolitical rivals.

In 2013, Edward Snowden, a contractor for the U.S. National Security Agency (NSA), leaked thousands of classified documents revealing the agency's extensive and unlawful mass surveillance of U.S. citizens, conducted using data obtained from major American telecommunications providers. Among the disclosures was a decision by the Foreign Intelligence Surveillance Court (FISC), which compelled Verizon to hand over all call detail records for communications both within the United States and between the U.S. and foreign countries.²⁰⁰ The leaked materials also showed that the NSA had spied on foreign officials. A report published by WikiLeaks alleged that the agency targeted over 125 phone numbers and intercepted the communications of senior German officials, including Chancellor Angela Merkel.²⁰¹ These revelations sparked global outrage, exposed deeply controversial surveillance practices, and significantly eroded public trust – both in the U.S. government and in the broader legitimacy of mass surveillance programs.

In North Macedonia, an illegal mass surveillance scandal posed a serious threat to the stability of the state and ultimately led to the fall of Prime Minister Nikola Gruevski. In 2015, the opposition released excerpts of more than 670,000 intercepted conversations spanning over 20,000 phone numbers that had been secretly recorded by Gruevski's administration between 2007 and 2013. The recordings, reportedly leaked by civil servants from within the system, revealed high-ranking officials discussing corruption, election fraud, and even murder cover-ups.²⁰² The scale and gravity of the scandal drew international attention and resulted in prison sentences of up to 15 years for six individuals, including the former Minister of Interior and a former intelligence officer who oversaw the wiretapping operation.²⁰³ The unprecedented scope of the surveillance and the explosive nature of the revelations once again propelled the issue of government overreach and unlawful surveillance into the global spotlight.

While public debates on state surveillance often center on security-based justifications rather than privacy concerns, practical evidence suggests that government agencies frequently operate beyond the boundaries established by legal frameworks. The case of Serbia illustrates how authorities can construct opaque surveillance infrastructures aimed at accessing user data held by telecom providers – often without the knowledge or oversight of the judiciary. As in many other countries, access to metadata or the covert interception of live communications is legally permitted under certain strict conditions, typically requiring a prior court order to ensure judicial oversight. However, because the formal process can be slow and evidentiary thresholds difficult to meet, authorities often bypass legal safeguards and approach mobile operators directly, effectively sidestepping judicial control.

In Serbia, alongside the formal request-and-approval mechanism that permits surveillance with prior court authorization, three parallel mechanisms have emerged in practice to enable government access to personal data. The first is a web-based application that allows independent access to retained data. Designed for convenience, it can be accessed using credentials provided by telecom operators and does not require a court order, thereby enabling unrestricted access to the operator's entire database. The second mechanism is exclusive to the national Security Information Agency (BIA), which receives daily transfers of user metadata from operators – regardless of whether the individuals concerned are under investigation or suspected of any criminal activity. The third and most far-reaching mechanism grants BIA a direct technical connection to the operator's infrastructure, enabling real-time interception of communications and unmediated access to all retained metadata.²⁰⁴ This case illustrates the extent to which government agencies may go in order to obtain user data and the parallel systems they develop to circumvent legal safeguards and judicial oversight.

As communication increasingly shifted from traditional channels, such as phone calls, to online platforms, states began to lose control over the flow of information. A growing share of conversations moved to private, encrypted applications, placing the content beyond the reach of law enforcement. This shift created the need for a new approach to interception – one that bypassed both mobile operators and encryption altogether. Achieving this required unprecedented access to the full contents of a target's device – not only calls and messages, but also deeply personal information such as photos, documents, browsing history, and the data of anyone whose information was stored on the device, regardless of their relevance to an investigation.

The rise of spyware signaled the beginning of a new era in digital surveillance – one that is significantly more invasive and far less constrained by oversight or accountability.



PRIVACY FATALISM AND THE NORMALIZATION OF DIGITAL SURVEILLANCE

The rapid evolution of technology has profoundly – and irreversibly – reshaped our understanding of privacy. In the past, individuals had greater agency in deciding whether to leave a digital trace; today, that choice has all but disappeared. Control over personal data has largely shifted away from individuals. Even those who consciously avoid smartphones or the internet remain subject to the pervasive collection of their personal data. Information related to education, health, employment, travel, marital status, and countless other aspects of life is routinely gathered, stored, and shared, often without explicit consent or even awareness. This widespread erosion of privacy violation aligns with Shoshana Zuboff's concept of *surveillance capitalism*, which argues that contemporary capitalist structures increasingly depend on extraction and commodification of personal data to operate and evolve.²⁰⁵ Much of the information collected is obtained without informed consent, and individuals are often unaware of the scale or purpose of its use. In such a system, privacy violations are no longer the exception – they have become structurally embedded and normalized.

Our physical movements are increasingly monitored through vast networks of surveillance cameras, while our digital behavior is continuously tracked by the technologies we depend on to communicate and participate in modern society. Smartphones, now essential to daily routines, simultaneously

function as powerful surveillance tools – running software that persistently collects, analyzes, and transmits personal data. Despite mounting concerns over privacy, tech industry leaders continue to promote the narrative that the benefits of innovation outweigh the associated risks. As a result, many individuals come to overlook – or even accept – the gradual erosion of privacy as an unavoidable trade-off. In this environment, privacy is no longer seen as a practical choice, let alone a societal priority.

This widespread resignation reflects a phenomenon known as *privacy fatalism* – the belief that individuals have little control over their personal data, regardless of their choices or actions.²⁰⁶ Closely tied to this is the normalization of digital surveillance, a process that both reflects and accelerates the erosion of privacy. States continue to expand surveillance infrastructures with limited pushback, often justifying their use by appealing to notions of security, public order, and administrative efficiency.

Repeated exposure to digital surveillance technologies – combined with prevailing narratives that frame them as tools for increased security – ultimately leads to their normalization.²⁰⁷ This process unfolds in different ways. Some individuals place considerable trust in state institutions and come to view surveillance as an added layer of protection. Others, deeply distrustful of the state, accept constant monitoring as an inescapable part of contemporary life. Still others adopt the mindset that they have “nothing to hide”, and therefore feel indifferent to the spread of surveillance technologies.

The global rise in government surveillance technologies is often accompanied by a wide range of actions, behaviors, and even cultural narratives used to justify their deployment. In China, digital surveillance has not only been normalized but has become a key mechanism in establishing individual social status. The country’s Social Credit System monitors citizens’ financial, social, moral, and political behaviors, assigning scores based on perceived trustworthiness. It aggregates data from diverse sources – including financial institutions, government databases, legal and administrative records, social media activity, and biometric surveillance systems – to determine a person’s overall score and grant access to public and private services.²⁰⁸

In London, the Metropolitan Police has progressively incorporated increasingly intrusive surveillance systems into routine policing, including

the use of live facial recognition cameras.²⁰⁹ According to a 2021 study on the most surveilled cities worldwide, London ranked as the most surveilled city in Europe and the sixth most surveilled globally.²¹⁰ This gradual integration of invasive technologies into everyday public spaces contributes to the normalization of surveillance – even in countries with established rule of law traditions such as the United Kingdom.

In Iran, digital surveillance functions as a key instrument of state repression, particularly in enforcing the country's Chastity and Hijab laws. Authorities employ video surveillance systems to monitor public spaces for violations of the mandatory dress code. When a violation is detected, police units transmit the location to field agents equipped with IMSI-Catchers – devices that intercept mobile signals and enable the identification of targeted women. The growing use of digital surveillance to enforce hijab compliance has been documented in multiple United Nations reports, underscoring the role of technology in reinforcing gender-based control.²¹¹

In the current era of advanced digital surveillance and a growing sense of privacy fatalism, states are increasingly working to normalize the use of highly intrusive technologies, including spyware. While public attention has largely shifted toward spyware, its deployment has been made possible by the earlier, gradual integration of other surveillance technologies into everyday life – laying the groundwork for more invasive tools to follow. The unprecedented ease of access to vast amounts of personal data has made spyware one of the most coveted instruments of state surveillance, particularly in jurisdictions where regulation targeting it remains weak or deliberately absent.

Despite claims that spyware serves national security interests, particularly in the prevention of crime and terrorism, there is no credible evidence or publicly available data to support its effectiveness in these domains. In practice, spyware has primarily been used as a tool of state repression, targeting activists, journalists, and human rights defenders. Whether developed by state or commercial vendors, spyware is inherently *intrusive by design*, posing a direct threat to fundamental rights and liberties.

Individuals targeted by spyware are subjected to a range of human rights violations including breaches of the right to private life and data protection, as well as the rights to freedom of expression, assembly, and association. Once installed on a device, spyware enables unrestricted access to all stored and transmitted data – private communications, documents, photos,

videos, contacts, financial information, and any other data processed through mobile applications.

Moreover, the intrusion extends beyond the primary target, violating the rights of all individuals whose personal information is present on the compromised device. This includes children, family members, lawyers, and journalistic sources – none of whom are formally subject to investigation.

Finally, the use of spyware has profound societal consequences. It contributes to a pervasive *chilling effect*, discouraging individuals from exercising their rights and liberties due to the fear of digital surveillance and the irreversible loss of privacy.²¹²

Despite its inherently harmful nature, the use of spyware has been documented across the globe, regardless of political system or level of democratic governance. Its global proliferation is driven by the rapid expansion of the spyware industry and the complicity of states that either deploy or enable its use. In response to growing demand, new and increasingly sophisticated commercial spyware tools continue to be developed. Today's surveillance market offers a broad spectrum of technologies, ranging from well-known commercial spyware such as Pegasus, Predator, and Graphite, to state-developed "knock-off" products like Serbia's NoviSpy, China's EagleMsgSpy, and Russia's Monokle. These tools are often supported by digital forensic technologies that facilitate their deployment, such as the UFED developed by the Israeli company Cellebrite.

State complicity in the proliferation of spyware is particularly damaging, not only because it legitimizes the use of intrusive technologies by governments, but also because it contributes to a spillover effect that normalizes their presence in the private sphere. *Stalkerware*, a form of spyware covertly installed on devices to monitor children or intimate partners, most often women, experienced a staggering 239% global increase in 2023.²¹³ Simultaneously, *bossware* (employee monitoring software), which gained traction during the COVID-19 pandemic as remote and hybrid work became widespread, has since become a standard practice in many workplaces around the world.²¹⁴

Whether deployed by authoritarian regimes or democratic governments, marketed as commercial products, developed covertly by intelligence agencies, or embedded within profit-driven surveillance platforms, these invasive technologies are systematically dismantling the foundations of

privacy and human dignity. No longer operating at the margins, they have become woven into the fabric of everyday life – silently tracking, profiling, and exploiting individuals across borders and cultures.

This normalization of digital surveillance risks ushering in a new era of repression, one where rights are eroded not through brute force, but through the quiet, pervasive use of technology. Left unchecked, this expanding regime of digital control threatens to redefine very meaning of freedom, reducing the human experience to one of constant observation, commodification, and control.



SPYWARE AS A SYSTEMIC THREAT TO HUMAN RIGHTS

This section argues that any use of spyware by state actors constitutes an unjustifiable overreach of government power. This position will be illustrated through a series of country examples that reveal how these technologies are deployed for a range of purposes – from national security claims to domestic political control. While the stated justifications may differ, the underlying concerns remain consistent: government use of spyware is inherently discriminatory, deeply invasive, and operates beyond meaningful legal accountability. In every instance examined, spyware has been used not as a neutral tool of justice, but as a mechanism for exerting control, suppressing dissent, and violating fundamental rights.

One of the foundational pillars of democratic societies is the trust between government institutions and the citizens they serve. Yet, over the past decade, this trust has significantly eroded, with numerous indicators pointing to a global decline in confidence in democratic governance.²¹⁵ Amid the rapid advancement of digital technologies, many governments have chosen to harness these tools in ways that are often more invasive than beneficial – frequently under the pretext of national security or public protection. This trend mirrors the broader expansion of mass surveillance infrastructures, which are increasingly normalized despite their serious implications for civil liberties.

At a time when core freedoms and democratic values are in retreat globally,²¹⁶ it is more critical than ever to ensure that governments are held accountable for how they deploy advanced technologies. According to the V-Dem Institute, approximately 72% of the world's population lived under autocratic rule in 2024, meaning nearly three out of four people are now subject to regimes with limited or no democratic safeguards.²¹⁷

Before turning to specific examples of how spyware is deployed, it is essential to outline the primary ways in which its use by governments undermines

public trust and safety around the world. This erosion occurs through three interrelated dynamics: (1) the inherently intrusive and discriminatory nature of spyware systems, (2) the flagrant and systemic violations of human rights, contravening standards set by international legal frameworks and human rights institutions, and (3) the cultivation of a chilling effect across societies.

Spyware as a highly intrusive and non-selective technology by default raises serious concerns regarding the violation of fundamental human rights. Its use consistently exceeds the boundaries of core legal principles of necessity and proportionality, making it incompatible with the values of a democratic society. Spyware is *intrusive by design*, enabling unauthorized access not only to a device but to the entirety of its stored and transmitted data. Unlike traditional surveillance methods that are subject to due process and judicial oversight, spyware operates covertly – without the knowledge or consent of the targeted individual – and grants operators unrestricted access to a person’s most intimate digital spaces, including messages, emails, photos, calls, geolocation, and even live microphone or camera feeds.

This intrusiveness is further magnified by spyware’s non-selective deployment and its frequent use outside legal frameworks and without public transparency. Rather than operating within systems of public oversight, spyware is typically deployed through secretive state or commercial channels that evade accountability. Once installed, it collapses the boundary between public and private life, rendering every interaction vulnerable to manipulation, blackmail, or repression. Its indiscriminate nature, combined with stealth and technical sophistication, transforms spyware into a weapon of mass surveillance that erodes democratic institutions, silences dissent, and discourages civic participation.

The human rights impact of spyware is both direct and indirect. At its most immediate level, the use of spyware constitutes a serious violation of the right to privacy and the protection of personal data – rights enshrined in key international and regional human rights instruments, including Article 8 of the European Convention on Human Rights (ECHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 7 of the Charter of Fundamental Rights of the European Union, and Article 12 of the Universal Declaration of Human Rights. As the Venice Commission has affirmed,²¹⁸ the deployment of spyware inherently interferes with these rights. Even though the ECHR does not contain a distinct right to data protection under the ECHR, the European Court of Human Rights has

consistently interpreted such protections as essential to safeguarding the broader right to privacy.

However, the harms caused by spyware are not limited to violations of privacy. By enabling access to an individual's entire digital ecosystem – including communications, documents, personal relationships, and professional networks – spyware is often deployed without regard for legal safeguards such as necessity, proportionality, or prior authorization. Its indiscriminate nature results in serious infringements of additional rights, including the rights to freedom of expression, association, and peaceful assembly; the right to a fair trial; the right to an effective legal remedy; and the right to work and freely choose one's occupation. Crucially, these violations extend beyond the primary target to include those in their proximity – confidential sources, clients, colleagues, family members, and even children. In such cases, third-party rights are routinely and unjustifiably compromised, often without the individuals concerned ever being notified or afforded any form of redress.²¹⁹

Additionally, the right to a fair trial is further undermined by the opaque nature of spyware deployment. Targeted individuals face almost insurmountable barriers to seeking justice due to the lack of transparency, independent oversight, and effective legal remedies. In many cases, the state – frequently the actor behind the surveillance – is also responsible for adjudicating complaints, raising serious concerns about impartiality and access to redress. Evidence indicates that individuals targeted by state-sponsored spyware are often subjected to pressure, intimidation, or coercion, leading them to alter their advocacy work, shift the focus of their reporting, or abandon their activities altogether. This constitutes a direct violation of the right to work and the freedom to choose one's occupation. In a democratic society, the work of activists, journalists, and civil society actors is essential. Protecting them from unlawful surveillance is not only a human rights obligation, but a prerequisite for preserving public accountability, free expression, and civic engagement.

In light of these realities, spyware cannot be regarded as a narrowly scoped law enforcement tool. Its deployment carries broad and often irreparable human rights consequences that strike at the core of democratic participation, civic space, and the integrity of information flows. A rights-based framework must therefore be central to all current and future discussions on spyware. Such a framework should prioritize transparency, accountability, strict legal

safeguards, and robust oversight mechanisms to effectively curb the use and abuse of these intrusive technologies.

A chilling effect arises when government actions deter people from engaging in legitimate activities such as protesting, exercising their rights, or expressing criticism of state institutions. The mere possibility of retaliation can serve as a powerful disincentive, leading people to self-censor or withdraw from public life altogether. In democratic societies, the ability to critique institutions, assemble peacefully, and express dissent are foundational elements of civic engagement and accountability.

The mere existence of spyware capabilities in the hands of governments, even if not actively deployed, can function as a powerful instrument of intimidation. The opaque nature of surveillance, combined with the absence of transparency and oversight, fosters a culture of fear in which people feel that they may be constantly monitored or recorded. This perception is not without basis: numerous investigations have revealed that spyware is frequently used not against genuine security threats, but against civil society actors, political opponents, and members of the press. The psychological toll of potentially being surveilled, paired with the very real consequences of retaliation – such as arrest, defamation, or loss of employment – constitutes an invisible yet pervasive form of repression. It undermines not only the right to privacy, but also the broader social and political conditions necessary for democratic participation and resilience.

As previously noted, no government – regardless of its political structure or guiding principles – can credibly claim to uphold democratic values while deploying highly invasive technologies to surveil its own population. Critics may argue that state-sponsored spyware is necessary for maintaining law and order, often citing its use in tracking terrorists and criminals. However, to date, there is no credible evidence that the use of spyware meaningfully enhances public security or improves the effectiveness of security agencies. Confronting the chilling effect of surveillance is not merely about safeguarding individual privacy; it is about protecting the foundational conditions in which democratic life can exist and flourish.

**A PRIVACY NIGHTMARE: UNDERSTANDING SPYWARE
PRACTICE SPYWARE AS A SYSTEMIC THREAT TO HUMAN RIGHTS**





THE MYTH OF JUSTIFIED SURVEILLANCE

The three dimensions outlined earlier – intrusiveness, human rights violations, and the chilling effect – are often best understood in the context of the type of government deploying surveillance technologies. A common assumption is that the use of advanced technologies is primarily a feature of authoritarian regimes, reflecting inherently repressive tendencies. However, research by SHARE Foundation conducted for the purposes of this study corroborated by other reports from security agency officials,²²⁰ reveals a more complex reality: nearly 100 countries worldwide have purchased and are actively deploying some form of advanced spyware. Notably, some of the most prominent commercial spyware vendors are based in countries widely regarded as democratic, including the United States, Germany, and Italy. Meanwhile, other countries – such as Israel – have adopted a more strategic approach, fostering an industry around the development and export of spyware as a tool for advancing geopolitical alliances and influence.²²¹

Despite the various arguments advanced to justify the use of spyware, its deployment consistently results in flagrant abuses of power and human rights, while fostering a global surveillance culture that threatens privacy and freedom of expression. By examining how spyware is used across various regimes and political systems – drawing both on classifications from leading indices such as Freedom House and V-Dem, and on patterns of deployment – the aim is to demonstrate that, regardless of the justification

offered, spyware invariably undermines human rights, erodes public trust in institutions, and constitutes a violation of the right to privacy. Across contexts, the outcomes are strikingly similar: journalists are surveilled and pressured, human rights defenders are threatened and intimidated, and societies as a whole become more digitally vulnerable and less free.



THE SECURITY ARGUMENT: THE ETHICAL-WASHING OF SPYWARE

Much like the justification for mass biometric surveillance, countries with strong rule-of-law traditions often defend their use of spyware by invoking national security. This framing effectively grants governments broad discretion to access individuals' private communications under the pretext of preventing terrorism, addressing transnational threats, or combating serious crimes such as child exploitation and organized crime. However, in practice, spyware has also been deployed by democratic governments to surveil activists, journalists, and other critics of power – actions that directly contradict the principles those governments claim to uphold. Notably, the international response to such abuses often varies depending on the perpetrating state. Democratic countries tend to face far less scrutiny or consequences, and within the European Union there is a troubling pattern of silence or inaction when autocratic regimes use spyware to target their citizens – even those residing within the EU.²²² Although the EU has positioned itself as a global leader in digital regulation, it continues to lag significantly in addressing the dangers of spyware. At present, there is neither comprehensive regulation nor a coherent forward-looking strategy for confronting the human rights risks posed by this technology.²²³

The rise in spyware use has paralleled the growing influence of populist and right-leaning political figures across Europe and beyond.²²⁴ These

political fractions often build their platforms around rigid policy agendas that prioritize anti-immigration measures, heightened securitization, and expanded government control. In such contexts, national security is frequently invoked as a justification for surveillance, yet the concept is often left deliberately vague. This ambiguity allows the term to be interpreted flexibly, enabling governments to tailor its meaning to fit shifting political objectives.

For example, the recent spyware case in **Italy** reflects a notable shift in how such technologies are used – and justified even within democratic countries. Italy has a long-standing history with spyware, having been the birthplace of Hacking Team, a company infamous for its ethically dubious products and indiscriminate sales practices. Hacking Team played a significant role in the early global proliferation of spyware technologies.

In early 2025, it was revealed that the Italian government had authorized the use of Graphite spyware against humanitarian workers assisting refugees and migrants crossing the Mediterranean Sea.²²⁵ The surveillance was officially justified as part of a counterterrorism operation, with the targeted individuals labelled as “potential threats to national security”.²²⁶ The revelations emerged after WhatsApp notified several individuals that their devices had been infected with military-grade software, typically reserved for use by government clients. The prevailing assumption, supported by circumstantial evidence, is that the software was deployed directly by the Italian government.

Notably, all of the targeted individuals had, at some point, publicly criticized Prime Minister Giorgia Meloni and her government’s policies,²²⁷ raising serious concerns about the political motivations behind the surveillance. The subsequent public backlash, along with criminal complaints filed by the targeted individuals,²²⁸ eventually led to Paragon, the Israeli company behind Graphite, terminating its contract with the Italian government. The company cited a breach of its terms of service as the reason for withdrawing.

The Italian case has reignited debate across Europe regarding the use of such technologies, though a clear and unified position on the issue remains elusive. As of February 2025, the European Commission had yet to present a comprehensive strategy to address the growing proliferation of spyware within the EU,²²⁹ despite the adoption of the final report by the PEGA committee – the European Parliament committee tasked with investigating the use of Pegasus – back in 2023.²³⁰ The prevailing response suggests that

these incidents are still being treated as isolated, nation-specific issues, rather than as part of a systemic problem affecting the Union as a whole. Although this is far from the first spyware scandal to shake the EU, the institutional pattern of inertia and fragmented response appears to be repeating itself.

The *Pegasus Project* constituted the largest global investigation into the use of spyware against politicians, journalists, and members of civil society. Across the cases uncovered, the common denominator was the involvement of state actors in the control and deployment of the spyware. In some instances, surveillance was conducted across borders, while in others governments used the technology domestically to monitor activists and critics within their own populations.

In 2019, a number of **Catalan** politicians and members of civil society and academia were targeted by the notorious NSO Group's *Pegasus*, as well as with surveillance technology sold by Candiru, another Israeli spyware vendor known for its covert ownership structure and exclusive dealings with governments.²³¹ Consequently, the Spanish government was widely presumed to be responsible for the attacks. Beyond these revelations, a separate investigation by Citizen Lab uncovered contracts between the Spanish government and private spyware vendors dating back to 2015. Notably, Spain's National Intelligence Center (CNI) was found to have engaged with Italy's Hacking Team on multiple occasions.²³² Surveillance technologies procured through these contracts were reportedly used to monitor Catalan individuals, including activists and Members of the European Parliament. The timing of the surveillance, which coincided with key political events between 2017 and 2020, strongly suggests that the operations were politically motivated and constituted a form of domestic espionage.²³³

The national security argument has been repeatedly evoked to justify the use of spyware, including in one of the most prominent European scandals in recent years – the 2022 **Greek** *Watergate* or *Predatorgate*. The case involved the covert surveillance of opposition politicians and investigative journalists by the Greek government, sparking widespread outrage and raising serious questions about the limits of executive power. Despite the establishment of a clear link between members of the ruling party and the targeting of devices with *Predator* spyware, the Greek Supreme Court ultimately cleared the National Intelligence Service (EYP) of any wrongdoing. Notably, before the verdict, both the head of the EYP and a senior government

official resigned and subsequently filed defamation lawsuits against media outlets that reported on the scandal. The acquittal of the state agency came despite credible evidence indicating EYP's involvement and what plaintiffs described as a flawed investigation and judicial process.²³⁴ Those targeted argued that the case exposed serious procedural irregularities and suggested that key evidence may have been overlooked to downplay the government's role. The trial also coincided with reports that the Greek Ministry of Foreign Affairs had authorized Predator export licenses to countries with poor human rights records, including Saudi Arabia, Madagascar, Bangladesh, and Sudan.²³⁵

Journalists and civil society actors are among the groups most at risk from surveillance and therefore require enhanced legal protections. In 2023, during negotiations on the new European Media Freedom Act (EMFA), it was revealed that several EU member states – including Greece, France, Italy, and Cyprus – were lobbying for loopholes that would allow surveilling journalists under loosely defined “national security” exemptions.²³⁶ While the EMFA presents an important step forward in reinforcing media freedom within the EU, it still falls short of affording robust safeguards against intrusive surveillance and spyware – particularly in countries with prior records of abuse, such as Greece and Hungary. Despite the participation of civil society and press freedom advocates, who raised concerns grounded in documented cases of misconduct, the final version of the act failed to fully align with international standards, including those set by the European Convention on Human Rights (ECHR).

In many cases, states develop a deployment narrative that emphasizes proportionality, due process, and minimal intrusion. **Canada**, for example, has publicly acknowledged the use of spyware as a tool for criminal investigations, even suggesting that such technologies have been employed as far back as 2002.²³⁷ Despite this rare admission, the Royal Canadian Mounted Police denied procuring or deploying Pegasus spyware and refrained from providing details about the specific cases in which surveillance tools were used. Nevertheless, the use of such software was justified as necessary to keep pace with evolving tactics employed by criminal organizations, particularly the use of encrypted communications.²³⁸ The muted public and institutional response to these disclosures highlights a broader inconsistency: while some countries are perceived as justified for using spyware under the banner of rule of law, others are condemned for

similar practices, reinforcing a double standard that obscures the systemic nature of the threat.

In another instance, the **German** Federal Criminal Police Office (BKA) justified its procurement and use of spyware by being restricted to cases involving terrorism and organized crime.²³⁹ While there have been no confirmed cases of German authorities using spyware to monitor or surveil civil society or human rights activists, serious questions remain: particularly regarding why the purchase of Pegasus was kept secret until the media exposed it. Internal reports indicate that BKA's legal experts had raised concerns about the intrusive capabilities of the software as far back as 2017,²⁴⁰ yet the agency proceeded with the acquisition.

Germany also played a significant role in the commercial spyware ecosystem through the FinFisher Group, developer of FinSpy, a surveillance tool capable of broad device control. In 2019, FinFisher was found to have exported its spyware to Turkey, a country with a well-documented record of human rights abuses, as well as several other Middle Eastern states.²⁴¹ The revelations prompted widespread public concern and ultimately led to criminal charges against the company's executives for violating EU export control regulation. Despite denying any involvement in the surveillance, torture, or imprisonment of civil society members based on data collected through FinSpy, the company eventually shut down after the German Public Prosecutor's Office froze its accounts and seized its assets – a rare win for privacy advocates in Europe.²⁴² However, it is important to note that this outcome was most likely enabled by two key factors: first, the legal action centered on export control violations, primarily financial in nature; and second, the case involved the transfer of spyware from a European company to repressive regimes outside the EU, which may have generated greater political will for enforcement.

Almost as a rule, these countries tend to acquire more sophisticated, commercially available spyware, most notably NSO's Pegasus. One likely reason is the way companies market their products: NSO, for example, promotes Pegasus as a precision instrument that only targets terrorists and criminals, and claims to work only with "military, law enforcement, and intelligence agencies from countries with good human rights records".²⁴³ Despite such justifications, governments remain reluctant to publicly acknowledge possession or use of these technologies. After Citizen Lab published its initial report mapping the global operations of Paragon

Solutions, **Australia** – alongside Canada, Cyprus, and Denmark – was identified as a possible customer of the company's highly intrusive software Graphite.²⁴⁴ While there is no confirmed evidence that the Australian government had used the spyware, examples from other countries that have procured Paragon's tools, such as Italy, underscore serious concerns raised by the invasive nature of such technologies.

Following the change of government in **Colombia**, newly elected President Gustavo Petro ordered an inquiry into the previous administration's purchase of Pegasus. The investigation revealed that the spyware had been acquired off the books and paid for in cash, strongly suggesting it was intended for surveilling journalists and opposition politicians.²⁴⁵ The use of surveillance technologies across Latin America has been extensively documented,²⁴⁶ often with severe consequences for those targeted and little to no institutional oversight. While Colombia is not exempt from these risks, it stands in a comparatively stronger position due to its ongoing push for greater transparency, stronger constitutional privacy protections, and a more independent judiciary.²⁴⁷ The clandestine nature of the NSO deal under the former Colombian government also raises broader concerns about the company's claims of ethical conduct and responsible sales practices.

Recent revelations from the *NSO Group v. WhatsApp* lawsuit have exposed a troubling new dimension of the company's operations. Contrary to NSO's claims that its government clients independently operate its tools, legal filings show that NSO itself controls key aspects of the deployment and data extraction processes.²⁴⁸ According to court documents, client governments need only submit a phone number – NSO staff then initiate and execute the surveillance from the company's own servers. This directly contradicts NSO's repeated defense that it merely licenses the software and holds no responsibility for its use. The revelation further damage the company's already dire human rights reputation, suggesting that NSO is not only a vendor of invasive surveillance tools, but also an active, unaccountable participant in global surveillance operations. Pegasus has already been used against journalists, human rights defenders, and political opponents around the world, often without legal oversight, consent or transparency. This creates a dangerous paradox: while NSO markets its software as a security solution aimed at protecting the public and combating crime, in reality it facilitates – and in some cases orchestrates – sophisticated spying operations that violate privacy, suppress dissent, and erode democratic freedoms. The recent U.S. court ruling in favor of WhatsApp/Meta, awarding nearly \$168

million in damages, marks a significant legal milestone, but also underscores the urgent need for coordinated international action to regulate, restrict, and ultimately prohibit the deployment of commercial spyware.



A SLIPPERY SLOPE TO AUTHORITARIANISM: WHY GOVERNMENTS NEVER STOP AT ONLY A COUPLE VIOLATIONS

Positioned between democratic and authoritarian systems, some regimes maintain a selective and strategic adherence to the rule of law, while preserving the appearance of democratic processes such as elections. In practice, however, these democratic elements are largely performative: power remains tightly concentrated in the hands of the ruling elite, elections are symbolic, the judiciary is politically aligned, and the media operates under heavy state influence. In such environments, state agencies – including the police and intelligence services – are often granted broad and unchecked authority to track, surveil, and interrogate anyone who challenges the government or expose corruption. Opposition politicians, civil society members, and activists are frequent targets, often monitored without justification or transparency. Marginalized communities and minority groups may also find themselves subject to disproportionate surveillance. These practices are rarely questioned and are often legitimized by vague and expansive interpretations of national security provisions, endorsed by both the courts and law enforcement institutions.

According to various reports, regimes that have partially or fully consolidated power are among the most active procurers and users of spyware – often sourced from companies based in democratic states.²⁴⁹ In

addition to utilizing well-known commercial surveillance systems, some of these governments have developed their own domestic versions of intrusive technologies. These homegrown systems allow intelligence and security agencies to customize their surveillance methods, making it easier to target critics and entrench political control. International responses to such practices are often inconsistent and appear to depend heavily on a country's geopolitical alignment. In many cases, condemnation is muted or absent altogether – particularly when internal political instability complicates diplomatic pressure or when strategic alliances override human rights concerns.

In 2021 and 2022, confirmed cases of Pegasus use in Hungary and Poland, both EU member states with increasingly illiberal governance, sparked debates within the European Commission and Parliament over the deployment of spyware within the bloc. The revelations followed a major leak that exposed a list of 50,000 phone numbers identified as potential surveillance targets across multiple countries, all linked to the NSO Group. The scandal led to one of the comprehensive investigations to date into the operations of the commercial spyware industry and triggered broader discussions on how states can prevent the misuse of these systems. Despite initially offering vague statements and showing little regard for democratic safeguards, the **Hungarian** government eventually acknowledged its use of the software, defending it as legal under national law. This admission enabled targeted Hungarian journalists to pursue a civil lawsuit. The broader fallout from the leaks included strong international responses, such as the blacklisting of NSO Group by the United States, and led to the creation of the PEGA Committee in the European Parliament, tasked with examining the impact of Pegasus and similar spyware within the EU.²⁵⁰

In 2024, **Poland** initiated an official investigation into the former ultraconservative government's use of Pegasus, which had reportedly been deployed against journalists and opposition politicians, including MEPs. While the complete list of targets has not been made public, the new government announced its intention to notify affected individuals in case they wished to pursue legal action or seek compensation. It remains unclear whether this commitment has been fulfilled. Notably, during its mandate, the right-wing Law and Justice (PiS) party undertook systemic overhaul of the judiciary, replacing judges and consolidating control over the police and intelligence services – measures that facilitated easier acquisition of court orders for surveillance purposes.²⁵¹ As part of the ongoing investigation,

Poland's former Justice Minister and the former head of the Internal Security Agency (ABW) were arrested in early 2025 on allegations of authorizing Pegasus surveillance against political opponents.²⁵²

Despite this, reports indicate that the PEGA Committee received limited cooperation from national authorities regarding the procurement and use of spyware within EU Member States. The predominant argument for this lack of engagement is the assertion that surveillance practices fall strictly within the remit of national sovereignty and therefore do not warrant broader European oversight.²⁵³ However, framing spyware use solely as a national matter poses significant challenges to the development of cohesive international standards aimed at curbing human rights violations and privacy intrusions facilitated by these technologies.

Mexico has experienced sustained and well-documented use of Pegasus spyware by military intelligence to target journalists, activists, and public officials, despite repeated public assurances to the contrary. Legal and institutional accountability remain weak, while persistent denials from the highest levels of government have only deepened the opacity surrounding these practices and hindered progress on digital rights. Although the Mexican government initially claimed that Pegasus was acquired to combat drug cartels and organized crime, subsequent investigations revealed its deployment against journalists, including those reporting on corruption and human rights abuses involving state actors.²⁵⁴

The scale and persistence of spyware deployment have positioned Mexico among the most extensively documented cases of abuse globally, with Pegasus repeatedly used to surveil civil society actors, particularly journalists, human rights defenders, and even government officials investigating state abuses. Despite official denials, forensic analyses by Citizen Lab and reports from civil society organizations have confirmed that the military intelligence agency (SEDENA) has used Pegasus spyware since 2019.²⁵⁵ Among the known targets are human rights defender Raymundo Ramos, surveilled while documenting military-linked extrajudicial killings in Nuevo Laredo;²⁵⁶ journalist Ricardo Raphael, whose devices were infected multiple times while investigating corruption and cartel infiltration of the state;²⁵⁷ and a journalist from *Animal Político* reporting on military abuses.²⁵⁸ Notably, surveillance also extended to Undersecretary for Human Rights Alejandro Encinas and members of the truth commission on the Ayotzinapa student disappearances, underscoring that Pegasus has not only been used

to monitor public dissent but also to undermine accountability efforts from within the government itself.²⁵⁹

This sustained targeting of civil society actors through military-grade spyware presents a serious threat to democracy and human rights. The surveillance of journalists undermines press freedom by fostering a climate of fear and self-censorship, especially when reporting on organized crime or government corruption. While the Mexican government continues to deny responsibility, leaked documents and FOI rulings have revealed that Pegasus contracts remained active under the current administration.²⁶⁰ In 2025, however, Mexico's attorney general launched a probe into allegations that former President Peña Nieto accepted nearly \$25 million in bribes from Israeli businessmen in exchange for government contracts involving spyware and other technologies, adding to the already damning case of unlawful spyware use.²⁶¹ With over 15,000 Mexican phone numbers appearing in the global Pegasus Project data leak, the country stands as a cautionary example of how unchecked surveillance technology can be weaponized against civil society, silencing dissent and eroding democratic accountability from both within and outside the state.

The latest Nagorno-Karabakh military conflict was identified as the catalyst for a widespread spyware operation targeting both Armenia and Azerbaijan. This case marks the first recorded instance of spyware being used for targeted surveillance in the context of an international armed conflict.²⁶² Azerbaijan, which has long maintained close ties with the Israeli government, had previously been identified as a client of the NSO Group. According to reports, at least 12 prominent Armenian figures, including journalists, human rights defenders, government officials, and UN personnel, had their devices infected with Pegasus during intense phases of the conflict.²⁶³ These infections coincided with key moments such as military escalations, ceasefire negotiations, and humanitarian crises, suggesting strategic surveillance aimed at undermining Armenia's diplomatic and informational resilience. Meanwhile, Azerbaijan was also found to have selected over 1,000 domestic phone numbers for potential targeting, with at least five confirmed Pegasus infections, including that of investigative journalist Khadija Ismayilova.²⁶⁴

The deployment of Pegasus in this conflict reveals another alarming dimension of its use – as a transnational weapon targeting civilians, diplomats, and humanitarian actors during wartime. Experts argue that such use violates international humanitarian law, which protects journalists

and civil society members in times of conflict. Anna Naghdalyan, a former spokesperson for the Armenian Foreign Ministry, warned that the surveillance may have compromised sensitive ceasefire communications, potentially influencing the course of negotiations.²⁶⁵ Organizations such as Access Now and the Council of Europe have called for urgent investigations and a global moratorium on the use of spyware in conflict zones, cautioning that the militarization of such technologies poses a grave threat to democratic institutions and the rules-based international order.

Southeast Asia has also emerged as a prominent Pegasus hub, with government critics frequently targeted by extensive spyware attacks. In **India**, journalists, judges, activists, and politicians were repeatedly subjected to surveillance, often in response to their criticism of the government. The Pegasus Project identified over 300 phone numbers linked to individuals in India – not confirming all as targets, but revealing a troubling pattern of infections and vulnerabilities.²⁶⁶ In response, the Indian Supreme Court launched a probe, which found evidence of spyware use but stopped short of explicitly linking it to Pegasus. The final report was withheld from the public, fueling uncertainty around the committee's conclusions.²⁶⁷ In 2025, the Court reaffirmed that the state's possession of spyware was not unlawful, citing national security, but acknowledged that surveillance of private citizens warranted further scrutiny. Nevertheless, it maintained that the report would remain classified due to security concerns.²⁶⁸

In 2022, it was revealed that the Thai government systematically cracked down on pro-democracy protests using a range of repressive measures, including spyware. While surveillance is already widespread in **Thailand**, the use of Pegasus during the 2020-2021 protests marked a significant escalation in the regime's tightening grip on civil liberties. Reports indicate that Thai authorities have been purchasing and using spyware to target civil society members for over a decade.²⁶⁹ In a rare legal challenge, a group of activists sued the government over the hacking of their phones; however, the civil court ultimately dismissed the case.²⁷⁰

Indonesia has also emerged as a prominent spyware hotspot. A 2024 report by Amnesty International's Security Lab uncovered a years-long, expansive network facilitating the import and export of surveillance technologies. The investigation revealed connections between Indonesian government agencies and several spyware firms, including NSO Group, Intellexa, FinFisher, and others.²⁷¹ Indonesia has repeatedly faced accusations of

fueling transnational tensions and of surveilling and suppressing domestic critics, contributing to an ongoing erosion of civic space.²⁷²

Serbia, classified as a hybrid regime and facing a steady decline in political rights and civil liberties in recent years, has a documented history of misusing surveillance technologies to target civil society and political opponents. From unauthorized access to citizens' retained metadata by state authorities and questionable attempts to legalize biometric surveillance, to credible allegations of spyware deployment, the Serbian government has consistently demonstrated its unreliability and lack of transparency in handling intrusive technologies. Since the early 2010s, state authorities have been linked to notorious spyware companies such as Hacking Team, Finfisher, Intellexa, and more recently, the NSO Group. Today, the use of spyware against activists, journalists, students, and the members of civil society appears to have become entrenched practice.

The deployment of Pegasus, widely considered the most sophisticated spyware currently available, has been documented in at least two cases in Serbia. In December 2023, two members of civil society received threat notifications from Apple, alerting them that they had been targeted by state-sponsored cyberattacks. Following verification of these alerts, SHARE Foundation, in collaboration with Access Now and Amnesty International, uncovered evidence of what appeared to be attempted Pegasus infections, likely exploiting vulnerabilities in the HomeKit functionalities of iPhone devices.²⁷³

The second case involved two investigative journalists from the Balkan Investigative Reporting Network – BIRN Serbia. They were targeted through custom Viber messages sent from an unknown number, claiming to offer information related to a potential story. The message included a malicious link that led to a website designed to mimic the well-known media outlet N1. Amnesty International later confirmed that the link was part of a one-click Pegasus infection attempt.²⁷⁴

In December 2024, an Amnesty International report uncovered the widespread use of a new type of spyware against activists, journalists, and members of civil society by the Serbian police and secret service.²⁷⁵ SHARE Foundation, with the support of Amnesty, identified a recurring pattern of spyware infections, ultimately confirming dozens of cases. The findings revealed that individuals – whether detained, abducted by police

or secret service agents, or voluntarily reporting a crime – had their phones confiscated or left unattended outside interrogation rooms. Without their knowledge, the devices were forcibly unlocked using a digital forensics tool known as UFED, developed by the Israeli company Cellebrite, and all stored and deleted data was extracted. After physical access was gained, the phones were then infected with domestically developed spyware dubbed NoviSpy, as confirmed by forensic evidence obtained by Amnesty Tech experts.

As outlined in the legal chapter, the use of spyware in Serbia is not only unlawful, but constitutes a criminal offense. Nevertheless, despite public backlash following the report – and denials from both the police and the secret service – the same surveillance practices have persisted. While spyware infections initially appeared to target high-value individuals, their deployment has since become increasingly opportunistic, demonstrating a blatant disregard for citizens' privacy.

In a separate briefing, Amnesty International highlighted another case involving the use of Cellebrite zero-day exploits to target the phone of a student participating in the mass student-led protests and blockades that have swept across Serbia since November 2024.²⁷⁶ The compiled reports and evidence are especially troubling given the scale of the protests and the simultaneous rise in both physical and digital repression. With large segments of the population mobilized in the streets, the reality in Serbia is that anyone can become a target of spyware.

Serbia stands out among hybrid regimes as the only known country to deploy domestically developed spyware. This is particularly notable given Serbia's lack of prior experience in developing advanced surveillance technologies. The emergence of NoviSpy raises serious questions, as its exact origins remain unclear. Circumstantial evidence points to two likely scenarios: either NoviSpy was developed in-house by Serbian security services through reverse engineering of more sophisticated tools like Pegasus or Predator, or it was created with technical support from foreign governments aligned with Serbian leadership. Russia and China, both close allies of Serbia, have developed their own domestic spyware – including Russia's Monokle,²⁷⁷ PlainGnome, and BoneSpy,²⁷⁸ and China's EagleMsgSpy –²⁷⁹ all of which share notable similarities with NoviSpy. Given Serbia's documented ties to Russia's FSB and previous procurement of Chinese surveillance equipment, it is highly plausible that NoviSpy was developed with foreign assistance. This possibility not only poses a serious threat to the rights of

Serbian citizens, but also signals the broader risk of deepening collaboration between declining democracies and authoritarian, or even totalitarian, regimes, particularly where close diplomatic relationships already exist.



SURVEILLED AND SENTENCED: WHEN YOU BECOME NOBODY'S PROBLEM

In autocratic regimes, spyware is not merely a tool of repression, but a cornerstone of governance. Unlike in democracies or hybrid regimes, where the public exposure of spyware use can trigger political fallout or public reckoning over government overreach, autocracies regard such tools as integral to their surveillance apparatus. These regimes often employ repressive methods indiscriminately across their populations to consolidate and maintain control. As a result, the use of spyware is less likely to generate public scrutiny or debate. Domestic cases are rarely publicized, and only when expat journalists or human rights defenders are targeted abroad do such stories break into international reporting. Another notable exception is when these regimes use spyware to target foreign actors or manage to acquire globally known technologies rather than relying on domestic alternatives.

In these political contexts, the deployment of spyware is not an exception but a routine extension of systemic repression. The ubiquity of censorship, restricted civic space, and the absence of independent oversight over security services ensures that state surveillance, whether covert or overt, is rarely contested domestically. As a result, the perception and visibility of spyware use differ substantially. Unfortunately, the absence of unambiguous international backlash against states known for employing such surveillance

strategies reinforces the perception that these regimes can act with impunity. Their deployment of spyware remains largely invisible and unchallenged. A closer examination of the autocratic surveillance arsenal reveals how spyware serves to entrench unaccountable power, extend repression beyond national borders, and ultimately destabilize global norms around privacy and sovereignty.

Autocracies frequently develop their own surveillance tools, in part to evade export controls. Russia, for example, avoids foreign spyware – reportedly due to deep-seated institutional paranoia – with its agencies even rejecting Pegasus in favor of domestic solutions.²⁸⁰ China has invested billions in proprietary surveillance technologies, including cameras, big data systems, and AI, making it effectively autonomous in digital espionage and enabling it to export these systems globally.²⁸¹ Similarly, Saudi Arabia and Egypt have built bespoke hacking capabilities tailored for domestic use. These self-sufficient programs demonstrate that banning foreign spyware vendors (as some governments have done with NSO Group) only scratches the surface: authoritarian states with sufficient resources can and do engineer their own spyware. In short, autocrats are not constrained by procurement barriers; they manufacture the digital weapons they need, intensifying human rights violations.

Russia has long employed spyware as part of its broader crackdown on human rights and liberties, targeting both domestic and exiled critics. Countless activists, opposition politicians, and independent journalists have been subjected to surveillance, often accompanied by physical harassment and intimidation. More recently, Russia's surveillance practices have escalated further, with a draft law proposing the mandatory installation of tracking applications on the devices of all foreign nationals in the Moscow region, supposedly to combat migrant-related crime.²⁸² Such a measure could set a dangerous precedent, opening new avenues for surveillance not only within Russia, but globally.

Persistent cases of state surveillance – such as the deployment of Monokle spyware, discovered on the returned device of a dissident previously confiscated by the Russian security service FSB,²⁸³ and other spyware such as PlainGnome and BoneSpy – ²⁸⁴ demonstrate how domestically developed spyware is used to maintain control even beyond state borders. Monokle is an Android spyware developed by the Russian defense contractor Special Technology Center, designed to extract extensive data from targeted devices.

The FSB has also developed and deployed bespoke surveillance software, some of which has been active for over two decades, targeting journalists, activists, and political exiles across Europe.²⁸⁵

The use of spyware in Russia remains poorly documented, largely due to the country's authoritarian structure and tight control over information flows. Independent investigations are often stifled, and transparency is minimal, making it difficult to ascertain the full scope of state surveillance. However, the limited revelations that do emerge offer a stark warning.

In **China**, spyware is a component of a multi-layered surveillance regime targeting both the general population and specific groups such as Uyghurs or Tibetans. Provincial security authorities have deployed spyware to extract text messages, audio recordings, and location data from citizens.²⁸⁶ These tools facilitate predictive policing and preemptive arrests, reinforcing a surveillance state that operates without accountability or transparency. Researchers have uncovered EagleMsgSpy, a powerful Android surveillance tool reportedly used by Chinese public security bureaus since at least 2017. Developed by Wuhan Chinasoft Token Information Technology, it requires physical access for installation and enables the recording and exfiltration of vast amounts of data.²⁸⁷

China's global spyware operations epitomize this trend. From installing spyware on tourists' phones at border crossings²⁸⁸ to targeting European businesses through the BRICKSTORM backdoor,²⁸⁹ Chinese authorities and affiliated actors treat cyberspace as a domain of strategic influence rather than rule-bound engagement. The flow of sensitive phone data through Chinese-controlled systems raises serious concerns about the geopolitical weaponization of surveillance.²⁹⁰

The Russian and Chinese cases demonstrate what happens when spyware technologies are left unchecked: surveillance becomes embedded in daily life, dissent is silenced through digital repression, and privacy is systematically dismantled under the guise of security and state control. Notably, some EU countries have also invoked national security to justify spyware deployment, failed to disclose their practices transparently, and have been caught targeting journalists and civil society members. In the end, the distinction often appears to be one of optics rather than principle.

Spyware use by autocratic regimes has a corrosive impact on global norms. It erodes state sovereignty by intruding on individuals' privacy across borders

and weakens digital rights frameworks grounded in consent, transparency, and accountability. Iran's deployment of spyware hidden in seemingly innocuous apps, such as games and restaurant guides, demonstrates how these tools can exploit user trust and erode autonomy.²⁹¹ Such practices not only violate digital ethics but also set dangerous precedents for the privatization and militarization of cyberspace.

Spyware transforms the digital landscape into a weaponized extension of autocratic rule. In 2011, **Bahrain** used the FinSpy spyware in 2011 to infiltrate the phones of activists based in the UK who were working on behalf of political prisoners back home. This led to a landmark UK Court of Appeal decision allowing two Bahraini dissidents to pursue legal action against the Kingdom, despite Bahrain's attempt to invoke sovereign immunity.²⁹² The case gained traction in the UK due to the recognition that the surveillance constituted a threat occurring on domestic soil as an instance of transnational repression. The UK v. Bahrain case marks a step in the right direction, demonstrating that states have both the responsibility and capacity to protect the rights of dissidents within their borders and to resist digital threats that often transcend national borders.

Morocco has similarly used Pegasus spyware to target journalists and human rights defenders. In one case, surveillance extended to journalists' families, spreading fear throughout their networks. Private information extracted from their devices was later weaponized – used to discredit them in pro-government media and even as evidence in court proceedings.²⁹³ The transnational nature of spyware amplifies its threat, allowing regimes to suppress dissent not only domestically but also across diasporas, undermining asylum protections and democratic safe havens. Notably, research suggests that the European Union supplied Moroccan authorities with surveillance technologies other than Pegasus for the stated purpose of combating “illegal migration”. However, evidence indicates that this spyware was also used to monitor journalists within the country.²⁹⁴ Another notable case involved the alleged targeting of Spanish PM Pedro Sánchez by Moroccan authorities. Although NSO Group's lack of cooperation stalled the investigation, the incident marked the first confirmed use of Pegasus against a European head of government and fueled diplomatic tensions between Spain and Morocco.²⁹⁵

Iran routinely weaponizes spyware to suppress protests and maintain control. Leaked documents reveal that during mass demonstrations,

authorities used spyware to track citizens' locations and contacts, facilitating mass detentions and intimidation. The domestic spyware system, known as SIAM, is operated by the Communications Regulatory Authority (CRA) and enables interception of communications as well as throttling of internet speeds – an especially potent tool during protests.²⁹⁶ By making private dissent visible to the state, such surveillance dismantles safe spaces for resistance and reinforces autocratic rule through fear. The system can also map activist and protester networks through mobile operator data. These revelations stem from leaked internal documents, including user manuals from an Iranian cellular carrier, and surfaced in the aftermath of the 2022 nationwide protests following the murder of Mahsa Amini. SIAM reportedly allows Iranian police to track protesters in real time and issue direct warnings, telling them to avoid participation in anti-government actions.²⁹⁷

Spyware's covert nature and lack of accountability mechanisms make it especially dangerous in autocracies, where virtually anyone can be deemed a legitimate target. Its unchecked proliferation erodes international norms and weakens democratic resilience, particularly as autocratic regimes export these technologies or inspire imitation elsewhere. The international community's to regulate the spyware industry, despite mounting evidence of abuse, further entrenches and normalizes authoritarian surveillance practices.

However, while Iran's and other countries' extensive abuse of spyware against their own activists has been well documented,²⁹⁸ – and regularly condemned by human rights groups – most governments reserve their strongest censure for cases that affect their interests. In practice, Western states have imposed export controls or blacklisted companies only when spyware has been used against their citizens or allied nations.²⁹⁹ Otherwise, strategic and economic ties often temper the response. This signals to autocrats that foreign surveillance of dissidents is unlikely to be punished – unless it strikes a geopolitical nerve.

The **Turkish** case exemplifies how autocracies exploit global surveillance markets to facilitate repression at home and abroad, often circumventing democratic norms and export controls. As previously mentioned, a criminal investigation initiated by Reporters Without Borders and other human rights and press freedom organizations in Germany led to charges against FinFisher executives for the illegal export of spyware to Turkey. The software

was allegedly used to monitor opposition figures and journalists, including those living abroad.³⁰⁰ The scandal ultimately resulted in FinFisher declaring bankruptcy and shutting down. While this case demonstrates how public pressure and legal action can be mobilized to push back against surveillance abuses, it also underscores the stark disparity in how spyware is treated in Western countries, such as the EU, Canada, and the U.S., compared to elsewhere, even when the supplier in question is a European company.

Saudi Arabia is likely responsible for one of the most notorious cases of spyware abuse, uncovered in the aftermath of the October 2018 murder of dissident journalist Jamal Khashoggi inside the Saudi consulate in Istanbul. The killing was swiftly linked to the Saudi regime and Crown Prince Mohammed bin Salman, largely due to Khashoggi's sustained and well-founded criticism of the Kingdom's policies. Subsequent investigations revealed that Pegasus spyware had been used to target individuals close to Khashoggi both before and after his murder. It was also uncovered that spyware was deployed in Turkey to monitor the investigation once Khashoggi's remains were discovered. Although NSO Group denied any direct involvement and no definitive link was established between Pegasus and the killing, Saudi Arabia had been a known client since 2017 – making it difficult to disentangle the company from the country's concerning human rights record, including extensive surveillance of critics. While NSO Group reportedly cancelled its contract with Saudi Arabia after Khashoggi's murder, later investigations revealed that the Israeli government encouraged NSO, Candiru, Cellebrite, and other domestic surveillance companies to continue selling to the Gulf state, downplaying human rights concerns. Some of these deals were signed even after Khashoggi's execution and the global backlash that ensued.

Despite widespread outrage, Saudi Arabia has faced little to no consequences for its repressive practices against dissidents. While the Khashoggi case triggered major international condemnation, the Saudi government has continued to surveil, intimidate, and silence critics. However, six years later, the UK High Court ruled in favor of Saudi human rights defender Yahya Assiri, allowing him to pursue a case against the Saudi government for targeting him with Pegasus between 2018 and 2020. This effort to confront the kingdom's transnational repression marks a necessary move toward curbing – and hopefully eradicating – the use of invasive surveillance technologies that can have fatal consequences.

Israel is a key player in both the development and global distribution of these technologies. By some estimates, it has more surveillance companies per capita than any other country in the world³⁰¹ and is the largest exporter of surveillance infrastructure globally, with nearly a third of countries sourcing advanced surveillance tools from companies based in or affiliated with Israel.³⁰² The commercial spyware sector in Israel maintains close ties to top government officials, facilitating deals with foreign governments. For example, Paragon Solutions Ltd. – founded in 2019 by former Prime Minister Ehud Barak and former IDF commander Ehud Schneorson –³⁰³ confirmed in early 2025 that it has sold its products to the U.S. government, reiterating its policy of working only with “a select group of global democracies”.³⁰⁴ Meanwhile, NSO Group, known for its production of Pegasus – the highly invasive spyware now almost synonymous with the targeting of journalists – has been at the center of multiple public scandals over the past five years.

This raises a critical question: how can countries that engage in egregious surveillance of their own citizens – as well as those in other countries where their operations extend – still be considered democracies? A 2018 study revealed that the Israeli and U.S. governments facilitated trainings and workshops in which U.S. police officers traveled to Israel for field visits. There, they met with military and law enforcement officials to learn about technologies and practices in use, particularly the deployment of surveillance tools against disenfranchised communities.³⁰⁵

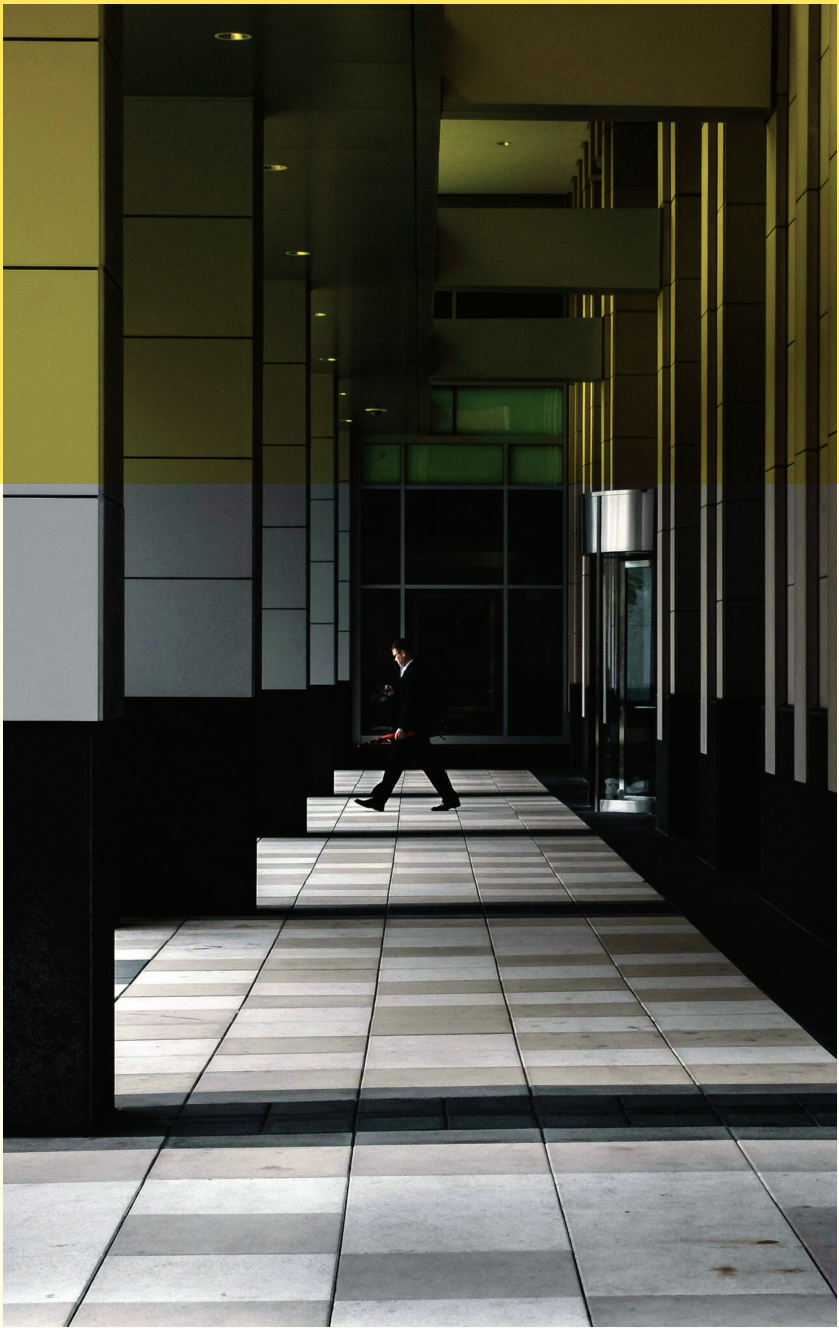
Human rights experts and organizations have long warned that the unchecked use of advanced technologies by governments in warfare would inevitably become a domestic issue. The concept known as the *imperial boomerang*,³⁰⁶ coined in 1950 by French author Aimé Césaire, suggests that repressive tools used to control colonized populations are ultimately redirected inward to control domestic populations. This has proven true in multiple cases: Israeli surveillance technologies first deployed against Palestinians have later been marketed and sold to other governments for use against their own citizens, while the NSA’s communication surveillance methods deployed in Afghanistan and the Bahamas, were eventually turned on American citizens and at U.S. borders.³⁰⁷

Israel is a distinct example of a country engaged in what is increasingly referred to as *spyware diplomacy* – the strategic use of surveillance technology exports to strengthen geopolitical alliances and advance foreign policy interests.

Sales of Israeli spyware are not merely commercial transactions but appear to be carefully calibrated, as reflected in company mission statements and the selective list of client states.³⁰⁸ This dual-use approach raises concerns on two levels: first, Israel has cultivated a multibillion-dollar industry centered on the export of cyber surveillance tools;³⁰⁹ and second, these tools are often “battle-tested” on Palestinians under occupation, effectively normalizing invasive surveillance practices without accountability.³¹⁰ In parallel, the Israeli government is currently reviewing a proposed bill – referred to as the “Spyware Law” – that would allow authorities to secretly access and monitor individuals’ personal data and communications without their knowledge.³¹¹ The draft legislation has already drawn sharp criticism from legal experts, judges, and human rights advocates, who warn it would grant the police unchecked surveillance powers.

There is ample evidence of a long-standing tradition of countries exchanging influence and tools to surveil their populations.³¹² As surveillance technology has become more sophisticated, it has also become easier for states to covertly engage in such forms of diplomatic relation-building. Yet, time and again, it has been proven that such arrangements rarely remain secret for long – eventually, the paper trails surface.

A comprehensive examination of spyware use across countries and regimes reveals a consistent pattern: spyware is primarily deployed to monitor dissent, not to protect public safety as often claimed. The argument that such tools can be justified within legal frameworks quickly unravels when confronted with real-world evidence. By design, spyware operates in secrecy, lacks accountability, and is prone to abuse. Whether deployed under the guise of democratic oversight or authoritarian command, its use undermines public trust, infringes on fundamental rights, and lays the groundwork for ever more intrusive forms of state control.



SPYWARE INC.

FROM THE ITALIAN JOB TO AN ISRAELI EMPIRE

What began as a niche technological solution has evolved into a billion dollar industry.³¹³ The global demand for increasingly sophisticated surveillance gadgets has surged alongside the digitization of communication, pushing law enforcement and intelligence agencies to seek tools capable of breaching encrypted platforms and bypassing traditional investigative methods. As a result, spyware development and sales have proliferated across jurisdictions, creating a competitive and largely opaque marketplace for digital intrusion – one that blurs the line between public safety and authoritarian overreach.

Following the early success of commercial spyware systems, global interest in their development skyrocketed. Research by the Atlantic Council mapped 435 entities in the spyware ecosystem as of 2023 – including vendors, investors, holding companies, intermediaries, and even individuals.³¹⁴ Given the rapid and secretive evolution of the industry, that number is likely even higher today. In such a fluid environment, regulatory oversight remains weak. Legal frameworks have consistently lagged behind technological innovation, enabling authorities to justify spyware deployment under vague or outdated provisions – or in some cases, to deploy it in outright violation of existing laws.

Although the spyware market today is often associated with Israel, its origins – and likely its future – are more complex and geographically diverse. While parts of the industry have since decentralized and taken root in the EU,³¹⁵ some of the earliest development in commercial spyware for state use in fact occurred in Europe itself. One of the first such companies, RCS Labs, was founded in 1992 and initially operated as a facilitator for Hacking Team's products.³¹⁶ It wasn't until 2019 that RCS Labs was directly linked to its own spyware tool, Hermit.³¹⁷ The most infamous Italian player in this field, however, was Hacking Team, established in 2003. The company's Remote Control System (RCS) was sold to a number of repressive regimes around the world. In 2015, a major hacking incident exposed over 400GB of internal

documents, including client lists and business practices, severely damaging the company's reputation.³¹⁸ In the aftermath, Hacking Team was acquired by cybersecurity firm Memento Labs in 2019, essentially undergoing a rebrand. Just a year later, David Vincenzetti declared the company "dead" in a LinkedIn post, bringing an almost two-decade legacy in state-sponsored surveillance to a close.³¹⁹

Italy's emergence as the birthplace of the global spyware industry was no coincidence. For centuries, the country has grappled with the presence of one of the world's most notorious and enduring criminal networks, the Italian mafia. Although the influence and violence of mafia groups have waned over time, this decline was in large part due to a forceful and sustained response by state authorities.³²⁰ The need for more effective tools to combat organized crime, coupled with a permissive legal environment that empowered security forces with broad investigative powers, created fertile ground for domestic cybersecurity companies to develop and distribute surveillance technologies.³²¹ In this context, Italy became an early incubator of the commercial spyware industry.

Another major player in the spyware industry, FinFisher – owned by Gamma Group – was established in 2008 in Germany and became best known for its FinSpy product. Although initially restricted to sales within the EU due to licensing requirements, FinSpy was later found in countries such as Turkey, Egypt, and Myanmar. This led to a criminal complaint, prompting the German Public Prosecutor's Office to seize FinFisher's accounts and charge its executives for violating export regulations.³²² During the period when Europe served as a central hub for spyware production, such cases demonstrated that accountability – though limited – was still possible. Today, with the market becoming increasingly decentralized and less bound by EU regulations and democratic oversight, spyware companies operate with far less scrutiny. Israel now dominates the industry, bolstered by its expansive military-industrial complex and the normalization of surveillance practices both in armed conflict and civilian life, making it a global epicenter for spyware development and distribution.

Israeli cybersecurity companies specializing in spyware development and distribution began to emerge in the early 2010s,³²³ though they did not attract significant global attention until several years later. As in the Italian case, Israel offered favorable conditions for the growth of a robust spyware industry. Since its founding in 1948, Israel's geopolitical position in the

Middle East has embroiled it in numerous armed conflicts – most notably its ongoing occupation of Palestinian territories. This has fostered a deeply entrenched securitization culture, exemplified by mandatory military service for both men and women, which has produced a steady pipeline of military-trained cybersecurity specialists. Talented individuals are often recruited into Unit 8200, Israel’s largest military intelligence division specializing in cyber operations, which has become a prominent incubator for the country’s burgeoning private cybersecurity sector.

According to available data, of the 2,300 Israelis who have founded 700 Israeli cyber firms, 80% are graduates of Unit 8200.³²⁴ The founders of Israel’s most notorious spyware companies – including the NSO Group, Intellexa Group, Paragon Solutions, QuaDream, and Black Cube – were either former Unit 8200 operatives or high-ranking military intelligence officials. Israel also maintains strong institutional links between its academic sector, government (particularly the Ministry of Defense), and the military. Many Israeli universities host dedicated cyber research centers that frequently carry out projects commissioned by the Ministry of Defense, the IDF, and major military contractors.³²⁵

With the IDF serving as the primary incubator for talent, Israeli spyware companies benefit from uniquely favorable conditions for development, testing, and distribution. Israeli control over Palestine territories offers access to millions of (unwilling) subjects, enabling real-world testing of various forms of weaponry, including digital surveillance tools. Once proven effective in the field, unburdened by privacy concerns, these tools are marketed as “battle-tested”, a feature that distinguishes Israeli spyware from competitors.³²⁶ Distribution is further aided by Israel strategic use of *spyware diplomacy*,³²⁷ and its enduring alliance with the United States, which often insulates it from political repercussions.³²⁸ Together, these conditions have not only fueled a flourishing industry but enabled Israel to establish a global spyware empire.

To understand the scale and impact of this phenomenon, extensive internal research into publicly documented cases of spyware use was conducted for the purposes of this study. The study systematically maps these cases to illuminate patterns of deployment, identify the actors involved, and expose the broader ecosystem sustaining digital repression across borders. The analysis documented the use of over 18 different spyware products – both commercially developed and state-made – targeting individuals in

over 98 countries. The research distinguishes between commercial spyware developed by private vendors for global distribution, and state-developed spyware, created by government authorities exclusively for domestic use, without intent for commercial sale. This distinction is critical: although the effects of spyware infections are similar regardless of origin, the risks associated with each production model differ significantly.

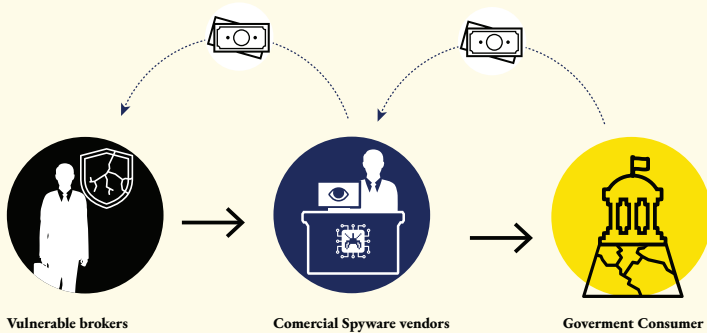
For example, commercial spyware is developed and sold for profit, with the objective of maximizing market reach and deployment. This profit-driven model fuels proliferation, as vendors compete to expand their customer base in an increasingly lucrative market. In contrast, state-developed spyware is produced internally by government entities, without third-party involvement. This absence of external collaboration reduces traceability and makes attribution significantly more difficult. Furthermore, without any form of independent oversight, such spyware can be deployed in complete secrecy, often with fewer constraints, enabling grave human rights violations while insulating state institutions from accountability. Although each model presents distinct risks, neither can be considered legitimate or justifiable.

The analysis found that of the 18 spyware products mapped, 8 are believed to be state-developed, while 10 originate from private vendors. These 10 were developed by prominent companies – 7 based in Israel, 2 in Italy, and one in Germany. Notably, the three most infamous spyware products – Pegasus, Predator, and Graphite – were developed by Israeli companies: NSO Group, the Intellexa Consortium, and Paragon Solutions. Among commercially available spyware, Israeli products consistently rank as the most sophisticated and effective, making them most sought-after by governments worldwide.



THE SPYWARE PROLIFERATION LOOP: VULNERABILITIES, VENDORS, AND STATE COMPLICITY

The spyware industry extends far beyond the companies that develop the tools themselves – it operates within a much larger and interconnected ecosystem. To remain both effective and profitable, spyware vendors depend on the vulnerabilities market to enable the covert deployment of their products, and on state authorities as their primary customers. Surrounding this core relationship is a wider network of actors: partner companies, suppliers, investors, brokers, and even independent researchers, all of whom play a role in sustaining this ecosystem. Collectively, they form a *spyware proliferation loop* or a self-reinforcing system in which every actor's role feeds the others. This dynamic not only maintains the industry's momentum, but also intensifies both the demand for intrusive surveillance tools and the incentives to develop and distribute them.



The first link in the spyware proliferation loop is the **exploitation of vulnerabilities**. Without these flaws, the covert deployment of spyware would be virtually impossible. Since the development of entirely secure systems remains out of reach – every piece of software contains potential weaknesses –³²⁹ this inherent insecurity has given rise to another lucrative industry: the vulnerabilities market.

Spyware companies typically follow one of two approaches to gain access to software vulnerabilities. Some, like the NSO Group, invest in internal research to independently discover and exploit these flaws. More commonly, however, companies purchase exploits from the global vulnerabilities market, where brokers, researchers, and hackers trade in zero-day and n-day vulnerabilities. Firms such as Crowdfense and Zerodium operate as intermediaries in this market, reselling discovered exploits to organizations and government contractors – purportedly for use in legitimate criminal investigations. In practice, however, these vulnerabilities often end up in the hands of commercial spyware vendors who incorporate them into surveillance tools they sell with little to no regard for how they are ultimately used. In 2024, Crowdfense reportedly offered between \$5 million and \$7 million for zero-day exploits targeting iPhones; up to \$5 million for zero-days targeting Android; up to \$3 million and \$3.5 million for Chrome and Safari zero-days, respectively; and \$3 million to \$5 million for zero-days affecting WhatsApp and iMessage.³³⁰

The prices continue to rise as big tech companies like Apple, Google, and Microsoft invest more resources into securing their devices and applications, thereby reducing the number of available exploits.³³¹ In its latest zero-day report, Google's Threat Intelligence Group (GTIG) tracked 75 zero-day

vulnerabilities exploited in the wild in 2024, down from 98 in 2023, with commercial spyware vendors leading in zero-day exploitation.³³²

Other actors in the vulnerabilities market, such as Trend Micro's Zero Day Initiative (ZDI), ethical hackers, independent researchers, and expert organizations also search for exploitable flaws.³³³ However, unlike those who sell to governments or commercial spyware vendors, these actors typically disclose vulnerabilities directly to the affected companies – either for a modest reward or on a pro bono basis – with the goal of ensuring they are patched before they can be exploited. Unfortunately, the vulnerabilities market remains heavily skewed in favor of exploitation, as governments and vendors offer significantly higher payouts, creating a strong incentive to prioritize offensive over defensive cybersecurity.

The second link in the spyware proliferation loop are **commercial spyware vendors** which are exploiting discovered zero-day and n-day vulnerabilities to build and deploy spyware products capable of infecting targeted devices.

As a global leader in the spyware industry, Israel has steadily built a sprawling machinery of spyware firms. As our initial research revealed, seven out of ten identified companies specializing in the development and sale of commercial spyware are based in Israel. These include the three most prominent names in the business – NSO Group, the Intellexa Consortium, and Paragon Solutions – as well as four less publicly known entities: Candiru, Circles, QuaDream, and BlackCube. Founded in 2010 by three former members of Unit 8200, NSO Group became Israel's first major spyware company and quickly rose to global prominence with its development of Pegasus, the most sophisticated spyware tool on the market. This intrusive spyware tool was made commercially available and covertly deployed by governments around the world for years, until a 2021 investigation by The Guardian and 16 partner media organizations revealed its widespread use in human rights violations, exposing the first major global spyware scandal.³³⁴ According to an internal NSO Group documents from 2016, The Guardian estimated the cost of Pegasus at €20.7 million per year to monitor 50 smartphones,³³⁵ making it a relatively expensive but highly effective tool of digital repression. In recent years, however, the growing number of commercial vendors and rising demand suggest that prices have likely decreased, making such tools more accessible than ever.

The second major spyware scandal surfaced in 2022, when Citizen Lab uncovered the use of Predator spyware to target Greek journalists

and opposition politicians.³³⁶ The case gained global attention in 2023 following an investigation by the European Investigative Collaborations (EIC) media network and Amnesty International's Security Lab in 2023, which revealed that Predator had been used by governments worldwide to unlawfully surveil activists, journalists, and government officials.³³⁷ The spyware's development was attributed to the Intellexa Consortium, a group of surveillance companies founded by a former commander of Israel's Unit 81, an elite intelligence corps.³³⁸ Although Intellexa operates under Israeli leadership and follows a typical Israeli surveillance business model, it was founded in Cyprus, a country that later emerged as a hub for the cyber-surveillance industry due to its lax regulatory environment and strategic location within the European Union. The companies that are part of the Intellexa Consortium are spread across Europe, including in Greece, Ireland, Hungary, and North Macedonia, with several entities named on the U.S. Commerce Department's blacklist.³³⁹ The North Macedonian company Cytrox was initially identified as the developer and deployer of the Predator spyware.³⁴⁰

The third and most recent spyware scandal, involving Graphite – a highly intrusive tool developed by the Israeli company Paragon Solutions – highlighted the unrelenting nature of the global spyware crisis and the strength of the spyware industry behind it. Founded by a former Israeli Prime Minister and a former commander of Unit 8200, Paragon Solutions sought to learn from the missteps of its predecessors by responding to growing pressure from civil society and anti-surveillance advocates. Graphite was marketed as a more “targeted” alternative, claiming to access only instant messaging applications rather than the full contents of a device, as Pegasus had. Furthermore, a senior executive publicly asserted that the tool would be sold exclusively to “countries that abide by international norms and respect fundamental rights and freedoms”, denying that non-democratic regimes would ever become clients.³⁴¹

However, as previously noted, spyware is by design a highly intrusive and indiscriminate tool of digital repression – fundamentally incompatible with democratic principles. Its continued use risks setting a dangerous precedent that could accelerate the erosion of human rights and civil liberties, even in established democracies. Despite assurances from spyware companies, a Citizen Lab report revealed that the Italian government had used spyware to target activists, journalists, and civil society organizations engaged in migrant search and rescue operations near the Italian coast, far removed

from its purported use in combating organized crime and terrorism.³⁴² The official response followed a familiar pattern: initial denial, followed by partial, cautious acknowledgment of spyware possession, accompanied by conflicting statements denying its use against civil society.

In response to the backlash following the 2021 Pegasus scandal – which placed Israel at the center of a growing industry implicated in serious human rights abuses – Prime Minister Benjamin Netanyahu pledged to tighten rules governing the export of offensive cyber tools. However, it was not long before reports emerged indicating that the Israeli administration was already considering easing those very restrictions.³⁴³ Despite numerous legal actions, including dozens of lawsuits against the NSO Group³⁴⁴ and other spyware vendors, the industry continues to thrive and expand into new global hubs.

With Israel formally tightening regulations on the export of offensive cyber tools, establishing and sustaining new commercial spyware vendors within the country became increasingly difficult. As a result, researchers and entrepreneurs began seeking alternative bases of operation. Barcelona emerged as one such hub, offering affordable, attractive living conditions comparable to Israel's, alongside substantial tax incentives under the Beckham Law – a special tax regime designed to attract foreign talent and high-earning professionals to Spain.³⁴⁵ Moreover, as a well-established European startup center alongside London, Amsterdam, and Berlin – Barcelona provides a fertile environment for the growth of the spyware industry. This shift was underscored in a TechCrunch interview with an Israeli security researcher, who disclosed being offered a position at a newly formed company, Palm Beach Networks, which was involved in everything from vulnerability exploitation to spyware development. Due to the dynamic nature of the spyware market, however, the company may have since changed its name or been absorbed into a different entity.³⁴⁶

Commercial spyware vendors frequently change their corporate identities and operating jurisdictions to evade legal accountability and avoid public scrutiny. At the same time, many cybersecurity researchers and experts move fluidly within the industry, often shifting roles from employees to founders of new spyware firms. According to data from the Atlantic Council, individuals in this sector are typically involved in two or more companies on average.³⁴⁷ This high degree of mobility fosters a fluid business environment

that enables the spyware industry to adapt and persist, even under mounting legal and societal pressure.

The most notorious commercial spyware vendors have not only inspired other private actors to enter the field of intrusive digital surveillance, but have also motivated certain state actors to attempt replicating the technology in-house. Our research indicates that these copycat spyware tools are most commonly found in autocratic regimes such as Russia, China, and Iran – with a possible spillover into Serbia, given its strong diplomatic ties with both Russia and China. For states lacking technologically advanced allies or the internal capacity to develop spyware, commercially available tools remain the only viable option. However, for those with sufficient expertise and resources, there are several reasons to pursue domestic development. First, strained diplomatic relations with countries where major spyware vendors are based can hinder procurement efforts. Second, ongoing democratic backsliding creates a permissive environment for opaque, unregulated spyware development and deployment. Finally, removing commercial vendors from the equation enables governments to manage surveillance operations more flexibly and discreetly. This shift toward in-house development could set a dangerous precedent – one that renders the spyware ecosystem even more opaque, decentralized, and difficult to regulate.

The third link in the spyware proliferation loop is the inherent **complicity of states** in the growth and expansion of an industry designed to egregiously violate fundamental human rights and liberties. State involvement in the spyware ecosystem operates on three levels. First, as outlined earlier in this chapter, governments have long sought to monitor and control their populations and spyware provides a powerful, modern means to do so in the digital age. The high cost associated with discovering and exploiting vulnerabilities, developing surveillance software, and managing its deployment have made spyware an expensive commodity. Yet the promise of persistent, covert, and far-reaching digital surveillance has made it a worthwhile investment for many governments – some of which deploy not just one, but multiple spyware tools. Through widespread procurement of spyware, often involving multimillion-dollar contracts, states not only sustain the commercial viability of the spyware market, but also drive demand for more advanced and harder-to-detect technologies. In some cases, governments even purchase vulnerabilities directly from brokers, bypassing commercial vendors, to fuel the development of in-house spyware.

Additionally, while some commercial spyware vendors advertise their products as undetectable, multiple high-profile scandals have revealed otherwise – placing certain governments at the center of global scrutiny. Despite mounting pressure from civil society and the public, state authorities routinely deny involvement, even in the face of compelling digital forensic evidence, or insist that such tools are used strictly for legitimate purposes such as combating crime or terrorism. However, the persistent absence of meaningful consequences, even when abuses are exposed abroad, points to a tacit understanding between government – a strategic code of silence that not only conceals current practices but also protects their own ability to use spyware in the future without accountability. As noted in the legal chapter, spyware continues to operate in a legal gray zone, with no binding international framework to prohibit or regulate its use. This lack of regulation offers state actors considerable leeway, reinforcing the political disinterest in pursuing stronger legal safeguards or meaningful oversight.

The spyware proliferation loop refers to a self-sustaining cycle in which commercial spyware vendors exchange technology for profit with both vulnerability brokers and government clients. This loop reveals a systemic, exploitative, and profit-driven approach to surveillance, bolstered by a vast network of stakeholders, including investors, partners, and individuals, who help normalize and privatize state and corporate control through intrusive technologies. Ultimately, the spyware proliferation loop exposes an expanding industry of digital repression and offers a stark warning about the future this trajectory may bring.

SPYWARE ON DEMAND: NEW TOOLS, OLD BEHAVIORS

Despite recurring scandals and widespread public condemnation, the commercial spyware industry continues to thrive.³⁴⁸ The proliferation of these technologies has made it alarmingly plausible for virtually anyone to acquire and deploy intrusive surveillance tools. What distinguishes spyware used in the private sphere from the state-deployed tools discussed so far is its commercial availability: it can be bought, sold, and used by anyone – against anyone. While much remains opaque about the broader commercial spyware market that fuels state abuse, two prominent forms of consumer-grade spyware have emerged: *stalkerware* and *bossware*.

These technologies make it easier than ever to collect and access information about others, whether intimate partners, children, or employees. Yet the underlying practice is hardly new: much like state surveillance throughout history, on demand spyware functions as a tool of control. The rise of state-deployed commercial spyware, combined with the inaction of regulatory authorities and a broader cultural shift toward the devaluation of privacy, has created ideal conditions for the spyware industry to thrive, particularly in the realm of private, consumer-level surveillance.



I ALWAYS SEE YOU: STALKERWARE AND PERSONAL RELATIONSHIPS

A PRIVACY NIGHTMARE: UNDERSTANDING SPYWARE
PRACTICE SPYWARE ON DEMAND: NEW TOOLS, OLD BEHAVIORS

Tools known as *stalkerware* enable anyone to surveil and collect information on others for an array of purposes. Defined as software that enables covert monitoring of a person's activity, these tools can be installed either remotely or through physical access to the target's device, where it blends in seamlessly and is difficult to detect.³⁴⁹ Stalkerware often include capabilities such as location tracking, access to messages and calls, microphone and camera activation, app usage monitoring, and keystroke logging. Most commonly, stalkerware is used to harass and control current or former intimate partners – hence the alternative term “spouseware” – and frequently constitutes one of the most pervasive forms of technology-facilitated gender-based violence.³⁵⁰

The digital age has introduced new anxieties around children's safety, prompting heightened vigilance among parents. Unlike older generations, who often lacked familiarity with online threats, today's parents are more attuned to digital risks, either because they grew up with technology themselves or because such concerns are now widely discussed, sometimes excessively.³⁵¹ This awareness fuels a growing reliance on surveillance apps to monitor children's communications and online behavior. Exploiting these fears, developers often market stalkerware as essential for child protection.³⁵² Yet even amid legitimate concerns, the covert use of such tools raises serious

ethical questions and constitutes a clear violation of children's rights, particularly their right to privacy. It also contributes to an increasingly surveilled daily life, reframing what safety and security mean in the digital age.

Unlike spyware targeting intimate partners, monitoring apps installed on children's devices are typically not uploaded covertly, and children are often aware of the oversight. In contrast, stalkerware used to surveil (ex) partners is frequently marketed in ways that leave little doubt about its intended use. The term *Intimate Partner Surveillance (IPS) spyware ecosystem*,³⁵³ a coined by Rahul Chatterjee and his colleagues, captures how these tools are not only widely accessible but also remarkably easy to install, operate, and hide from targeted persons. While some apps are misused for IPS despite not being designed for it, a growing number are created specifically for this purpose. According to Kaspersky's annual stalkerware report, 195 different stalkerware apps were detected in 2023.³⁵⁴

Despite the intrusive nature of commercial spyware for private use and its detrimental impact on fundamental human rights, particularly those of vulnerable groups such as survivors of physical and digital abuse (most of whom are women), as well as children, additional risks stem from frequent and large-scale data breaches. Since 2017, at least 25 stalkerware companies have experienced hacking attacks and significant data leaks, with some targeted multiple times.³⁵⁵ Most notably, mSpy, one of the most widely used stalkerware apps, suffered a breach that exposed the data of approximately 2.4 million customers, revealing sensitive information about both the users and their surveillance targets.³⁵⁶ Further, a 2022 TechCrunch report uncovered a vast network of stalkerware apps harvesting sensitive data of at least 400,000 people, all vulnerable to a major security flaw.³⁵⁷

In response to the rise of the spyware-on-demand industry, a global Coalition Against Stalkerware (CAS) was formed in 2019 through the joint effort of more than forty partners, including civil society organizations, IT security companies, academic institutions, law enforcement agencies, and others. The coalition's goal is to combat the growing threat posed by stalkerware.³⁵⁸ Its work, along with mounting public pressure, has contributed to several key developments. In 2023, the New York Attorney General secured a \$410,000 fine from Patrick Hinchey and 16 stalkerware companies, while also establishing a requirement that targeted persons be notified when their devices have been compromised.³⁵⁹ In a landmark decision, the U.S.

Federal Trade Commission also banned the Android app company Support King and its CEO Scott Zuckerman – developers of SpyFone app – from operating in the surveillance business.³⁶⁰

However, despite some progress in parts of the world, stalkerware continues to pose a significant threat to individual privacy and security. Addressing this issue requires legal, technological, and gender-sensitive perspectives. Just as narratives of privacy fatalism must be challenged, so too must the patriarchal norms that legitimize the surveillance of intimate partners. The majority of people targeted by stalkerware are women, many of whom are surveilled without their knowledge. Others may appear to consent under pressure or coercion, yet consent given under duress is not genuine consent.³⁶¹ Ultimately, stalkerware exemplifies broader concerns associated with spyware technologies: it is intrusive by design and fundamentally incompatible with human rights principles. For that reason, it cannot be justified – whether used by the state or private individuals.



SPYWARE AT WORK: HOW SURVEILLANCE TOOK OVER THE OFFICE

Another spyware-on-demand tool that has surged in popularity, especially during and after the COVID-19 pandemic due to the shift to remote work, is *bossware*.³⁶² This software allows employers to monitor employees' activity and productivity, sometimes with consent, but often covertly. Much like stalkerware, the surveillance capabilities of bossware are extensive: many programs can access all data on a device and track nearly every user action, including app and website usage, communication metadata, mouse and keyboard activity, secret activation of microphone and cameras, periodic screenshots, or even live screen video feeds.³⁶³ Some tools, such as Time Doctor and WorkSmart, are visible to employees and make the monitoring known. Others, like Teramind and StaffCop, are designed to be virtually undetectable.³⁶⁴

Even with the rise of bossware – including the listing of over 550 “labor-focused technology products” in the Bossware and Employment Tech Database compiled by Coworker in 2021 –³⁶⁵ the legality of such technologies remains contested. While regulations like the GDPR aim to safeguard individual privacy, effective oversight is often lacking or unevenly enforced across jurisdictions. Even where legal frameworks exist, data protection laws frequently have limited applicability within the workplace.³⁶⁶ In jurisdictions with stricter regulations requiring disclosure of employee

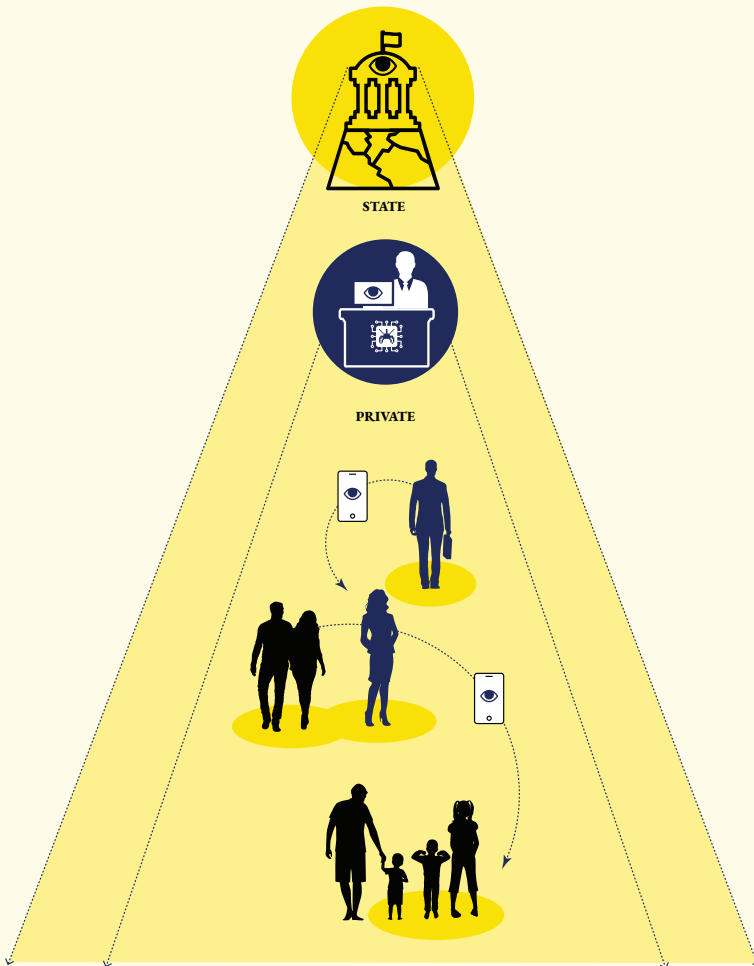
monitoring, such notices are often buried in lengthy contracts and obscured by legal jargon.³⁶⁷ Moreover, in many cases, withholding consent may not be a viable option, as employees risk reprimand or termination if they refuse to accept surveillance.

As established, bossware collects vast amounts of data on employees. While specific tools vary in function, most are designed to optimize productivity, reduce corporate liability, and enhance organizational security.³⁶⁸ Given the scale of investment in such technologies, it is reasonable to assume that monitoring data informs critical decisions – such as performance evaluations, promotions, demotions, and layoffs – thus contributing to the dehumanization of the workplace. Still, it remains debatable whether bossware meaningfully improves worker performance.³⁶⁹ Although one might argue that measurable gains in productivity could justify its use, evidence increasingly suggests the opposite: bossware tends to erode employee trust, heighten the sense of constant surveillance, and contribute to the automation and alienation of work – ultimately undermining productivity and morale.

The global rise in worker surveillance mirrors the patterns seen in other types of spyware and results in significant human rights violations, most notably the right to privacy. Research links the use of bossware to heightened levels of stress, anxiety, fear, depression, and a general decline in employee mental health.³⁷⁰ While bossware stems in part from legal stagnation and rapid technological development, it is also a symptom of capitalist ideologies taken to an extreme – prioritizing business optimization and profit over human dignity and rights, often leaving workers with little ability to opt out. Surveillance tends to become further normalized during periods of crisis, when security concerns are used to justify intrusive measures – a dynamic often described as *disaster capitalism*.³⁷¹ Ultimately, the spread of bossware forces a deeper reckoning: one that challenges prevailing notions of productivity and autonomy, and calls for a critical examination of how surveillance is increasingly used as a mechanism of control in the modern workplace.

The growing use of stalkerware and bossware reflects a troubling spillover of state surveillance practices into private and professional life. As governments normalize intrusive technologies in the name of security, these tools increasingly permeate homes and workplaces, used by intimate partners, parents, and employers alike. This diffusion blurs the lines between public

and private surveillance, steadily eroding expectations of privacy and personal autonomy. If left unchecked, such trends risk fostering a society where constant monitoring becomes the norm rather than the exception – redefining relationships, labor dynamics, and even personal identity through the pervasive lens of control.



BEYOND THE CONCLUSION

By Milica Jovanović

It is frighteningly easy today to make a compelling case against the proliferation and use of spyware technologies. The evidence is damning: invasive digital tools have been used to infiltrate phones, track movements, record conversations, and silently surveil journalists, activists, and political opponents across continents. And while some may argue that those public challengers of power have voluntarily engaged in political struggles, spyware has also been turned against the unsuspecting – people unprepared for the military-grade assault on privacy that defines today's surveillance landscape. High-tech overpolicing is already increasingly entrenched in marginalized communities, including racial and ethnic minorities, low-income neighborhoods, and historically over-surveilled urban areas. Migrants, asylum seekers, and displaced persons are routinely subjected to biometric tracking and predictive risk profiling through expanding border control regimes. Different in form but akin in purpose, such practices echo spyware's core function: to watch, to profile, to control. Most alarming, this surveillance architecture is not confined to rogue actors or authoritarian regimes; it is purchased, deployed, and justified by democratic governments and influential corporations, rendering spyware a standard tool within the apparatus of control in both liberal and illiberal systems.

This hunger for control – disguised as safety, framed as necessity – is nothing new. Throughout human history, rulers have sought to see, to know, and to preempt dissent, believing that visibility ensures stability. The tension between liberty and security, between personal autonomy and state oversight, is a deeply rooted feature of political life – not a novelty of the digital age.

Few thinkers have left a more lasting mark on this dilemma than Plato, a foundational figure in Western political thought. In *The Republic*, his earnest effort to imagine a just society, Plato offers a vision that today reads startlingly authoritarian: censorship of art and speech, the abolition of private property, all under the rule of a small elite of philosopher-kings. Yet this was a sincere philosophical attempt to cure what he saw as the moral and political disorder of his time, embodied most vividly in the execution

of Socrates and the decline of Athenian democracy. For Plato, individual liberty was not an end in itself, but a potential source of chaos if unmoored from virtue and wisdom. Order, harmony, and justice required that some freedoms be curtailed, not arbitrarily, but under the stewardship of those uniquely fit to understand and pursue the common good.

In this light, *The Republic* is less a utopia than a warning: when society is unwell, even noble ambitions can justify uncomfortable solutions. Plato's philosopher-kings, endowed with insight and clarity, bear an uncanny resemblance to today's algorithmic governors and technocratic overseers, those who claim the right to manage societies based on superior access to data, code, and predictive power. The question persists: who gets to define the good, and at what cost to the freedom of others?

By contrast, the liberal tradition that emerged centuries later placed individual freedom at the center of political legitimacy. Thinkers from Locke to Mill argued that the role of the state was not to mold virtue, but to protect autonomy and property, and to secure the freedom of thought and expression. Liberty, rather than state-molded virtue, became the foundation of justice. Yet this tradition is not without its blind spots. The liberal defense of freedom often presumes a level playing field, overlooking how structural inequality, coercive market forces, or opaque technologies can constrain choice as surely as any law. Moreover, in the digital age, the language of liberty is frequently invoked not to empower the public but to shield powerful actors from regulatory scrutiny, democratic oversight, or ethical accountability. Just as not every appeal to security is a smokescreen for repression, not every invocation of freedom is a pledge of justice.

Unfettered liberty can conceal systems of inequality, permit exploitation, or erode the institutions that sustain civic trust. In our digital age, calls for freedom of expression, innovation, or autonomy have at times been co-opted to avoid accountability, undermine regulation, or defend monopolistic control of information systems. The rhetoric of liberty can mask both surveillance capitalism and state neglect – two faces of unregulated digital power.

In other words, neither “security” nor “liberty” exists in a moral vacuum. Both can serve justice or subvert it, depending on who wields them, to what end, and with what safeguards. The spyware debate must be framed within this tension, not outside it. The danger lies not in acknowledging that states have legitimate security concerns, but in accepting unaccountable and

opaque methods as the default tools to address them. Equally, the defense of liberty must be more than a slogan; it must reckon with the realities of harm, exploitation, and asymmetry that unchecked freedom can entail.

What emerges from this historical arc is not a simple opposition but a perennial tension. Liberty and security are not binary choices but competing values that must be held in dynamic balance. Treating either as sacrosanct, whether the demand for perfect safety or the ideal of absolute freedom, risks eroding the very conditions that make democratic life possible. Spyware technologies embody the worst outcomes of this imbalance: tools of extraordinary reach, justified in the name of protection, yet designed to operate in secrecy, without oversight, and often beyond remedy. To oppose them is not to dismiss the state's responsibility to ensure safety, but to insist that security must be accountable, proportionate, and governed by public ethics, not private contracts or invisible code. Likewise, to defend liberty is not to romanticize it, but to recognize that meaningful freedom depends on structures that protect the vulnerable, constrain power, and prioritize transparency over convenience. In this light, the issue is not whether spyware can be used "safely", but whether a society committed to democratic values can afford to normalize its use at all.

Ultimately, the case against spyware is not merely technical or legal. It is a civilizational choice about the kind of society we are willing to build.

ENDNOTES

- 1 "If It's Smart, It's Vulnerable", <https://www.ifitssmartitsvulnerable.com/>
- 2 "Malware", Meriam-Webster.com Dictionary, <https://www.merriam-webster.com/dictionary/malware>
- 3 "Malware", US NIST Computer Security Resource Center, <https://csrc.nist.gov/glossary/term/malware>
- 4 In cybersecurity, confidentiality, integrity and availability are often referred to as the "CIA Triad". For more, see: "What Is The CIA Triad?", Fortinet, <https://www.fortinet.com/resources/cyberglossary/cia-triad>
- 5 Kurt Baker, "The 12 Most Common Types of Malware", Crowdstrike, February 27, 2023, <https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/>
- 6 "Spyware", US NIST Computer Security Resource Center, <https://csrc.nist.gov/glossary/term/spyware>
- 7 "Spyware and state abuse: The case for an EU-wide ban", European Digital Rights, 2025, p. 3, https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf
- 8 Ibid., p. 4
- 9 Ibid., p. 5
- 10 Ibid., pp. 6-7
- 11 Madeline Earp, "Forensic Tools Open New Front for Using Phone Data to Prosecute Journalists", GIJN, January 6, 2023, <https://gijn.org/stories/forensic-tools-open-new-front-for-using-phone-data-to-prosecute-journalists/>
- 12 "Spyware and state abuse: The case for an EU-wide ban", European Digital Rights, 2025, pp. 7-8, https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf
- 13 "Maltego", <https://www.maltego.com/>
- 14 "Magnet Griffeye", <https://www.magnetforensics.com/products/magnet-griffeye/>
- 15 "What Is Spyware?", Fortinet, <https://www.fortinet.com/resources/cyberglossary/spyware>
- 16 "What Is Spyware? Types, Risks, and Prevention Tips", SentinelOne, December 11, 2022, <https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-spyware/>
- 17 Ibid.
- 18 Amber Bouman, "More than 21 million employee screenshots leaked from WorkComposer workplace surveillance app", Tom's Guide, April 23, 2025, <https://www.tomsguide.com/computing/online-security/more-than-21-million-employee-screenshots-leaked-from-workcomposer-workplace-surveillance-app>
- 19 "What is spyware and what can you do to stay protected?", Amnesty International, December 14, 2023, <https://www.amnesty.org/en/latest/campaigns/2023/12/what-is-spyware-and-what-you-can-do-to-stay-protected/>
- 20 Bill Marczak et al., "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild", Citizen Lab, September 13, 2021, <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>
- 21 Andre Meister, "Prüfbericht zum BKA-Staatstrojaner: Die Software ist ████████"

- □□□□□□, Netzpolitik, February 21, 2022, <https://shorturl.at/AXzpj>
- 22 James Mackenzie, "What is Israel's secretive cyber warfare unit 8200?", Reuters, September 18, 2024, <https://www.reuters.com/world/middle-east/what-is-israels-secretive-cyber-warfare-unit-8200-2024-09-18/>
- 23 "A Zero Day that went undiscovered for 18 years", Black Hat Middle East and Africa, August 16, 2025, <https://insights.blackhatmea.com/a-zero-day-that-went-undiscovered-for-18-years/>
- 24 "What Is An Exploit?", Fortinet, <https://www.fortinet.com/resources/cyberglossary/exploit>
- 25 Bill Marczak et al., "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild", Citizen Lab, September 13, 2021, <https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>
- 26 "Surveillance Industry Glossary", Amnesty International Security Lab, <https://securitylab.amnesty.org/glossary/>
- 27 Ibid.
- 28 "Shodan", <https://www.shodan.io/>
- 29 "Censys", <https://censys.com/>
- 30 Bill Marczak et al., "Hacking Team and the Targeting of Ethiopian Journalists", Citizen Lab, February 21, 2014, <https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/>
- 31 Morgan Marquis-Boire et al., "Police Story: Hacking Team's Government Surveillance Malware", Citizen Lab, June 24, 2014, <https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/>
- 32 Morgan Marquis-Boire, Bill Marczak, "From Bahrain With Love: FinFisher's Spy Kit Exposed?", Citizen Lab, July 25, 2012, <https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/>
- 33 "German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed", Amnesty International, September 25, 2020, <https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/>
- 34 Bill Marczak et al., "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware", Citizen Lab, December 16, 2021, <https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/>
- 35 Bill Marczak et al., "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations", Citizen Lab, March 19, 2025, <https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/>
- 36 "What Is Social Engineering?", Proofpoint, <https://www.proofpoint.com/us/threat-reference/social-engineering>
- 37 Threat Analysis Group (TAG), "Buying Spying: Insights into Commercial Surveillance Vendors", Google, February 2024, p. 2, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf
- 38 Although GSM (Global System for Mobile Communications) technically refers to a family of standards for 2G (second generation) digital cellular networks, the term "GSM" is still commonly used as a generic label for subsequent generations of mobile phone technologies (3G, 4G, 5G) or even for mobile phones in general due to the widespread adoption of the original standard.

- 39 "Invisible Infrastructures: Surveillance Architecture", SHARE Lab, March 9, 2015, <https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/>
- 40 "Retention of communication data in Serbia: How much are we under surveillance? (2014–2016) [Zadržavanje podataka o komunikaciji u Srbiji: Koliko smo pod nadzorom? (2014–2016)]", SHARE Lab, August 29, 2017, <https://labs.rs/sr/zadrzavanje-podataka-o-komunikaciji-u-srbiji/>
- 41 Recent investigations into law enforcement surveillance at large-scale public events such as the 2024 Democratic National Convention in Chicago, have revealed evidence consistent with the deployment of cell site simulators. Researchers observed unusual cellular tower behavior, including unexpected IMSI requests followed by abrupt disconnections, which align with techniques used to identify and track protest attendees without clear legal authorization. Dhruv Mehrotra, "Secret phone surveillance tech was likely deployed at 2024 DNC", Wired, January 10, 2025, <https://www.wired.com/story/2024-dnc-cell-site-simulator-phone-surveillance>
- 42 "What is end-to-end encryption (E2EE)?", IBM, September 22, 2021, <https://www.ibm.com/think/topics/end-to-end-encryption>
- 43 Moxie Marlinspike, "Advanced cryptographic ratcheting", Signal Blog, November 26, 2013, <https://signal.org/blog/advanced-ratcheting/>
- 44 Steve Morgan, "Apple's CEO On Encryption: 'You Can't Have A Back Door That's Only For The Good Guys'", Forbes, November 21, 2015, <https://www.forbes.com/sites/stevemorgan/2015/11/21/apples-ceo-on-encryption-you-cant-have-a-back-door-thats-only-for-the-good-guys/>
- 45 Jen Roberts et al., "Markets matter: A glance into the spyware industry", Atlantic Council, April 22, 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/markets-matter-a-glance-into-the-spyware-industry/>
- 46 Casey Charrier et al., "Hello 0-Days My Old Friend: A 2024 Zero-Day Exploitation Analysis", Google Threat Intelligence Group, April 2025, p. 4, <https://services.google.com/fh/files/misc/2024-zero-day-exploitation-analysis-en.pdf>
- 47 "IMEI Check Service", <https://www.imei.info/>
- 48 Bill Marczak et al., "Predator in the Wires: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions", Citizen Lab, September 23, 2023, <https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/>
- 49 "Tech Guide: Detecting NoviSpy spyware with AndroidQF and the Mobile Verification Toolkit (MVT)", Amnesty International, December 16, 2024, <https://securitylab.amnesty.org/latest/2024/12/tech-guide-detecting-novispy-spyware-with-androidqf-and-the-mobile-verification-toolkit-mvt/>
- 50 "Surveillance Industry Glossary", Amnesty International Security Lab, <https://securitylab.amnesty.org/glossary/>
- 51 "Apple Platform Security", Apple, December 2024, https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf
- 52 "Secure an Android device", Android Open Source Project, <https://source.android.com/docs/security/overview>
- 53 "What is root access?", Fasthosts, November 1, 2023, <https://www.fasthosts.co.uk/blog/what-is-root-access/>
- 54 Threat Analysis Group (TAG), "Buying Spying: Insights into Commercial Surveillance Vendors", Google, February 2024, p. 29, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_

[Commercial_Surveillance_Vendors_-_TAG_report.pdf](#)

- 55 "Remote Code Execution (RCE)", Rapid7, <https://www.rapid7.com/fundamentals/what-is-remote-code-execution-rce/>
- 56 "Sandbox escape", NordVPN, <https://nordvpn.com/cybersecurity/glossary/sandbox-escape/>
- 57 "What Is Privilege Escalation?", Proofpoint, <https://www.proofpoint.com/us/threat-reference/privilege-escalation>
- 58 "Mercenary mayhem: A technical analysis of Intellexa's PREDATOR spyware", Cisco Talos, May 25, 2023, <https://blog.talosintelligence.com/mercenary-in-tellexa-predator/>
- 59 Ivan Righi, "Common Malware Loaders", ReliaQuest, 13 August 2024, <https://reli-aquest.com/blog/common-malware-loaders/>
- 60 "Mercenary mayhem: A technical analysis of Intellexa's PREDATOR spyware", Cisco Talos, May 25 2023, <https://blog.talosintelligence.com/mercenary-in-tellexa-predator/>
- 61 "What Is An Attack Surface?", Fortinet, <https://www.fortinet.com/resources/cyberglossary/attack-surface>
- 62 "What Is An Attack Vector?", Fortinet, <https://www.fortinet.com/resources/cyberglossary/attack-vector>
- 63 thaddeus e. grugq (@thegrugq), X.com (formerly Twitter), February 7, 2015, <https://x.com/thegrugq/status/563964286783877121>
- 64 "Social engineering", US NIST Computer Security Resource Center, https://csrc.nist.gov/glossary/term/social_engineering
- 65 "Journalists targeted with Pegasus spyware", Amnesty International Security Lab, March 27, 2025, <https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware/>
- 66 "Forensic appendix: Pegasus zero-click exploit threatens journalists in India", Amnesty International Security Lab, December 28, 2023, <https://securitylab.amnesty.org/latest/2023/12/pegasus-zero-click-exploit-threatens-journalists-in-india/>
- 67 "Operation Triangulation", Securelist by Kaspersky, <https://securelist.com/trng-2023/>
- 68 Boris Larin, "Operation Triangulation: The last (hardware) mystery", Securelist by Kaspersky, December 27, 2023, <https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/>
- 69 Bill Marczak et. al, "BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?", Citizen Lab, March 9, 2018, <https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/>
- 70 Bill Marczak et. al, "PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions", Citizen Lab, September 22, 2023, <https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/>
- 71 Sondas Asem, "Egypt: US blacklists Canada's Sandvine for technology targeting activists", Middle East Eye, February 27, 2024, <https://www.middleeasteyenews.net/news/us-blacklists-canadian-company-over-technology-used-human-rights-abuses-egypt>
- 72 "Predator Files: Technical deep-dive into Intellexa Alliance's surveillance prod-

- ucts", Amnesty International, October 6, 2023, <https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/>
- 73 Ibid.
- 74 "Cellebrite UFED", <https://cellebrite.com/en/ufed/>
- 75 Boris Babović, "Spyware's First Step: A Systematic Analysis of Exploits Used for Mobile Device Compromise", SHARE Foundation, May 29, 2025, <https://sharefoundation.info/en/spywares-first-step-a-systematic-analysis-of-exploits-used-for-mobile-device-compromise/>
- 76 "'A Digital Prison': Surveillance and the Suppression of Civil Society In Serbia", Amnesty International, December 16, 2024, p. 41, <https://www.amnesty.org/en/documents/eur70/8813/2024/en/>
- 77 Ibid, p. 75
- 78 Ibid, p. 76
- 79 "Cellebrite zero-day exploit used to target phone of Serbian student activist", Amnesty International, February 28, 2025, <https://securitylab.amnesty.org/latest/2025/02/cellebrite-zero-day-exploit-used-to-target-phone-of-serbian-student-activist/>
- 80 "Cellebrite Statement About Amnesty International Report", Cellebrite, February 25, 2025, <https://cellebrite.com/en/cellebrite-statement-about-amnesty-international-report/>
- 81 "'A Digital Prison': Surveillance and the Suppression of Civil Society In Serbia", Amnesty International, December 16, 2024, p. 30, <https://www.amnesty.org/en/documents/eur70/8813/2024/en/>
- 82 Ibid, p. 31
- 83 David Stevanović, "NoviSpy Exposed: Tracing Government-Linked Surveillance in Serbia", SHARE Foundation, May 29, 2025, <https://sharefoundation.info/en/novispy-exposed-tracing-government-linked-surveillance-in-serbia/>
- 84 Cooper Quintin, Rebekah Brown, John Scott-Railton, "Something to Remember Us By: Device Confiscated by Russian Authorities Returned with Monokle-Type Spyware Installed", Citizen Lab, December 5, 2024, <https://citizenlab.ca/2024/12/device-confiscated-by-russian-authorities-returned-with-monokle-type-spyware-installed/>
- 85 "Lookout Discovers New Chinese Surveillance Tool Used by Public Security Bureaus", Lookout Threat Lab, December 11, 2024, <https://www.lookout.com/threat-intelligence/article/eaglemsspy-chinese-android-surveillanceware>
- 86 Muawya Naser, Hussein Al Bazar, Hussein Abdel-Jaber, "Mobile Spyware Identification and Categorization: A Systematic Review", Informatica 47, no. 8 (2023): 45–56, pp. 47–48, <https://informatica.si/index.php/informatica/article/view/4881/2472>,
- 87 "Mobile Verification Toolkit (MVT)", <https://docs.mvt.re/en/latest/>
- 88 "AndroidQF", <https://github.com/mvt-project/androidqf>
- 89 "Tech Guide: Detecting NoviSpy spyware with AndroidQF and the Mobile Verification Toolkit (MVT)", Amnesty International, December 16, 2024, <https://securitylab.amnesty.org/latest/2024/12/tech-guide-detecting-novispy-spyware-with-androidqf-and-the-mobile-verification-toolkit-mvt/>
- 90 "GrapheneOS", <https://grapheneos.org/>
- 91 Mishaal Rahman, "How many software updates do iPhones get", Android Authority, February 26, 2025, <https://www.androidauthority.com/iphone-soft->

- ware-support-commitment-3449135/
- 92 C. Scott Brown, "Here are the phone update policies from every major Android manufacturer", Android Authority, April 15, 2025, <https://www.androidauthority.com/phone-update-policies-1658633/>
- 93 "Learn when you'll get software updates on Google Pixel phones", Google, <https://support.google.com/pixelphone/answer/4457705?hl=en>
- 94 Will Sattelberg, Anu Joy, "Here's every Samsung phone, tablet, and wearable that will get four years of Android updates", Android Police, May 11, 2024, <https://www.androidpolice.com/samsung-four-year-update-list-android/>
- 95 "About Apple threat notifications and protecting against mercenary spyware", Apple, April 23, 2025, <https://support.apple.com/en-us/102174>
- 96 "Threat Analysis Group", Google, <https://blog.google/threat-analysis-group/>
- 97 "Government-backed attack alerts", Google, <https://support.google.com/a/answer/9007870?hl=en>
- 98 "BlastDoor for Messages and iMessage", Apple, May 7, 2024, <https://support.apple.com/sr-rs/guide/security/secd3c881cee/web>
- 99 "About Lockdown Mode", Apple, April 9, 2025, <https://support.apple.com/en-us/105120>
- 100 Google, "Use Google Play Protect to help keep your apps safe & your data private", <https://support.google.com/googleplay/answer/2812853?hl=en>
- 101 "Mainline", Android Open Source Project, <https://source.android.com/docs/core/ota/modular-system>
- 102 Il-Sung Lee, "Advanced Protection: Google's Strongest Security for Mobile Devices", Google Security Blog, May 13, 2025, <https://security.googleblog.com/2025/05/advanced-protection-mobile-devices.html>
- 103 "About Project Zero", Google Project Zero, <https://googleprojectzero.blogspot.com/p/about-project-zero.html>
- 104 "What is Samsung Knox?", Samsung, <https://www.samsung.com/uk/mobile-phone-buying-guide/what-is-samsung-knox/>
- 105 "Protecting users from spyware", WhatsApp, <https://faq.whatsapp.com/641700318302674>
- 106 Constitution of Croatia, https://narodne-novine.nn.hr/clanci/sluzbeni/1998_01_8_121.html
- 107 Act on the Implementation of the GDPR, https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html
- 108 Act on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities, <https://www.zakon.hr/z/1061/zakon-o-zastiti-fizickih-osoba-u-vezi-s-obradom-i-razmjenom-osobnih-podataka->
- 109 Electronic Communications Act, https://narodne-novine.nn.hr/clanci/sluzbeni/2022_07_76_1116.html
- 110 Criminal Code, <https://www.zakon.hr/z/98/kazneni-zakon>
- 111 Cybersecurity Act, https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html
- 112 Criminal Procedure Act, <https://www.zakon.hr/z/174/zakon-o-kaznenom-postupku>
- 113 Ordinance on the Method of Conducting Special Investigative Measures, https://narodne-novine.nn.hr/clanci/sluzbeni/2009_08_102_2639.html

- 114 Basic Law for the Federal Republic of Germany, https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html
- 115 Civil Code, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html
- 116 Criminal Code, Division 15, https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1922
- 117 Federal Data Protection Act, https://www.gesetze-im-internet.de/englisch_bdsch/
- 118 Telecommunications-Telemedia Data Protection Act, <https://www.gesetze-im-internet.de/ttdsch/>
- 119 G10 Act, https://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html
- 120 Code of Criminal Procedure, https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html
- 121 Greek Constitution, https://www.hellenicparliament.gr/UserFiles/ebooks/ekdo-seis/2019_THE-CONSTITUTION-OF-GREECE/4/index.html
- 122 Greek Law 3917/2011, <https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/n-3917-2011.html>
- 123 Greek Law 5002/2022, <https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022>
- 124 EU Data Retention Directive, <https://eur-lex.europa.eu/eli/dir/2006/24/oj/eng>
- 125 General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- 126 Law Enforcement Directive (LED), <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>
- 127 Greek Law 4624/2019, <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>
- 128 Greek Law 4624/2019, <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>
- 129 Greek Penal Code, <https://www.kodiko.gr/nomothesia/document/529099/nomos-4619-2019>
- 130 Greek Law 5002/2022, <https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022>
- 131 Constitution of Guatemala, <https://constitutionnet.org/sites/default/files/Guatemala%20Constitution.pdf>
- 132 Constitutional Court of Guatemala, Expediente 1356-2006, <https://gt.vlex.com/vid/423896454>
- 133 Decree 21-2006 (Organized Crime Law), https://mingob.gob.gt/wp-content/uploads/2020/10/10_LeyContraDelincuenciaOrganizada.pdf
- 134 Access to Public Information Law of Guatemala, Decree 57-2008, http://www.congreso.gob.gt/detalle_pdf/decretos/13082
- 135 Law on Money Laundering and the Cybercrime Law of Guatemala (Decree 39-2022),
- 136 Digital Personal Data Protection Act of India, <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>
- 137 Indian Information Technology Act of 2000, https://www.meity.gov.in/static/uploads/2024/03/ITbill_2000.pdf
- 138 Indian Information Technology Act of 2000, <https://www.meity.gov.in/static/up->

- loads/2024/03/ITbill_2000.pdf
- 139 Indian Code of Criminal Procedure, https://www.indiacode.nic.in/bit-stream/123456789/15272/1/the_code_of_criminal_procedure,_1973.pdf
 - 140 Constitution of Indonesia, <https://jdih.bapeten.go.id/unggah/dokumen/peraturan/116-full.pdf>
 - 141 Human Rights Law (Law No. 39/1999) of Indonesia, <https://peraturan.bpk.go.id/Details/45361/uu-no-39-tahun-1999>
 - 142 Law No. 27 of 2022 on Personal Data Protection (PDP Law) of Indonesia, <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
 - 143 The Law on Electronic Information and Transactions of Indonesia (EIT Law, as amended by Law No. 19/2016) , <https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023>
 - 144 Penal Code of Indonesia, <https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023>
 - 145 Annisa Febiola, 2025, Dubai's EDGENX to Invest US\$ 2.3 bn in Indonesian Data Center Construction, https://en.tempo.co/read/2019618/dubais-edgnex-to-invest-us2-3bn-in-indonesian-data-center-construction?tracking_page_direct
 - 146 Law No. 27 of 2022 on Personal Data Protection (PDP Law) of Indonesia, <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Indian Telegraph Act of 1885, https://www.indiacode.nic.in/bit-stream/123456789/13115/1/indiantelegraphact_1885.pdf
- 147 Constitution of Ireland, <https://www.irishstatutebook.ie/eli/cons/en/html>
 - 148 European Convention on Human Rights, https://www.echr.coe.int/documents/d/echr/convention_ENG
 - 149 European Convention on Human Rights Act 2003, <https://www.irishstatutebook.ie/eli/2003/act/20/enacted/en/print.html>
 - 150 EU Charter of Fundamental Rights, https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng
 - 151 EU General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
 - 152 EU Law Enforcement Directive (LED), <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>
 - 153 Data Protection Act 2018, <https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html>
 - 154 European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, <https://www.irishstatutebook.ie/eli/2011/si/336/>
 - 155 Communications (Retention of Data) (Amendment) Act 2022, <https://www.irishstatutebook.ie/eli/2022/act/25/enacted/en/html>
 - 156 Criminal Justice (Offences Relating to Information Systems) Act 2017, <https://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/html>
 - 157 Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, <https://www.irishstatutebook.ie/eli/1993/act/10/enacted/en/print>
 - 158 Criminal Justice (Surveillance) Act 2009, <https://www.irishstatutebook.ie/eli/2009/act/19/enacted/en/html>
 - 159 Protection of Privacy Law of Israel <https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf>

- 160 Protection of Privacy Law of Israel <https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf>
- 161 European Commission, Adequacy decisions, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- 162 Criminal Procedure (Enforcement Authorities – Communication Data) Law of Israel, https://www.law.co.il/en/news/2007/12/18/new_law_regulates_access_to_communication_data/
- 163 Constitution of Mexico, <https://www.scjn.gob.mx/sites/default/files/cpeum/documento/cpeum.pdf>
- 164 National Code of Criminal Procedures of Mexico, <https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf>
- 165 National Guard Act of Mexico, <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf>
- 166 National Security Ac of Mexicot, <https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf>
- 167 Federal Law for the Protection of Personal Data in Possession of Obligated Parties of Mexico, <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>
- 168 Federal Law for the Protection of Personal Data in Possession of Private Parties of Mexico, <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- 169 Federal Criminal Code of Mexico, https://www.oas.org/juridico/spanish/mex_res13.pdf
- 170 Ejército Espía, <https://ejercitoespia.r3d.mx/>
- 171 Organic Law of the General Public Administration of Mexico https://www.oas.org/juridico/spanish/mex_res4.pdf
- 172 General Law of the National Public Security System of Mexico, http://dof.gob.mx/nota_detalle.php?codigo=5076728&fecha=02/01/2009
- 173 Law of the National Public Security Investigation and Intelligence System of Mexico, https://www.dof.gob.mx/nota_detalle.php?codigo=5763160&fecha=16/07/2025
- 174 General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- 175 Constitution of the Republic of Poland, <https://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm>
- 176 Police Act, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19900300179/U/D19900179Lj.pdf>
- 177 Criminal Code, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf>
- 178 Constitution of Serbia, https://www.paragraf.rs/propisi/ustav_republike_srbije.html
- 179 Personal Data Protection Act, https://www.poverenik.rs/images/stories/dokumentacija-nova/zakon-o-zastiti-podataka-o-licnosti_en.pdf
- 180 Law on Electronic Communications, <https://www.paragraf.rs/propisi/zakon-o-el-ektronskim-komunikacijama.html>
- 181 Criminal Procedure Code, <https://mpravde.gov.rs/files/CRIMINAL%20PROCEDURE%20CODE%20%202019.pdf>
- 182 Criminal Code, <https://www.mpravde.gov.rs/files/Criminal%20%20%20>

Code_2019.pdf

- 183 Constitution of Spain, <https://www.senado.es/web/conocersenado/normas/constitucion/detalleconstitucioncompleta/index.html?lang=en>
- 184 Criminal Procedure Act of Spain, <https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf>
- 185 General Data Protection Regulation (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- 186 Law Enforcement Directive (LED), <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>
- 187 Spanish Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>
- 188 Spanish Organic Law 7/2021, <https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806>
- 189 Criminal Procedure Act (Ley de Enjuiciamiento Criminal, LECRIM), <https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf>
- 190 Spanish Law 9/2014 on Telecommunications, <https://www.wipo.int/wipolex/en/legislation/details/15762>
- 191 Spanish Law 34/2002 on Information Society Services and E-Commerce (LSI-CE), <https://www.wipo.int/wipolex/en/legislation/details/20419>
- 192 Privacy International, Right to Privacy in Turkey, https://privacyinternational.org/sites/default/files/2017-12/UPR_Turkey_0.pdf
- 193 Turkish Criminal Code, <https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/tr/tr171en.html>
- 194 Turkish Civil Code, <https://rm.coe.int/turkish-civil-code-family-law-book/1680a3bcd4>
- 195 Turkish Personal Data Protection Law, <https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf>
- 196 Report by the European Commission, https://enlargement.ec.europa.eu/document/download/8010c4db-6ef8-4c85-aa06-814408921c89_en?file-name=T%C3%BCrkiye%20Report%202024.pdf
- 197 Freedom House, "Freedom on the Net 2024: The Struggle for Trust Online", 2024. <https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online>.
- 198 Amnesty International, "Global: 'Predator Files' spyware scandal reveals brazen targeting of civil society, politicians and officials", October 9, 2023 <https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/>.
- 199 Susan Landau, "Surveillance or Security? The Risk Posed by New Wiretapping Technologies", Massachusetts Institute of Technology, 2010, p. 23.
- 200 Ewen Macaskill and Gabriel Dance, "NSA Files: Decoded", The Guardian, November 2013. <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>
- 201 "NSA tapped German Chancellery for decades, WikiLeaks claims", The Guardian,

- July 2015. <https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel>
- 202 Joanna Berendt, "Macedonia Government Is Blamed for Wiretapping Scandal", The New York Times, June 2015. <https://www.nytimes.com/2015/06/22/world/europe/macedonia-government-is-blamed-for-wiretapping-scandal.html>
- 203 "N Macedonia: 6 ex-officials get prison terms for wiretaps", Associated Press, February 2021. <https://apnews.com/general-news-bfa470426a071f4d-f2642dfd21342442>
- 204 "Invisible Infrastructures: Surveillance Architecture", SHARE LAB, March 2015. <https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/>
- 205 Shoshana Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", Profile Books, London, 2019.
- 206 Evan Selinger and Hyo Joo Rhee, "Normalizing Surveillance", SATS, vol. 22, no. 1, 2021, pp. 49–74. <https://doi.org/10.1515/sats-2021-0002>
- 207 Ibid.
- 208 F. Liang, V. Das, N. Kostyuk, and M. M. Hussain, Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure, Policy & Internet 10(4) (2018), pp. 415–453, https://www.researchgate.net/publication/326817957_Constructing_a_Data-Driven_Society_China's_Social_Credit_System_as_a_State_Surveillance_Infrastructure
- 209 "London Police Make 540 Arrests Using Live Facial Recognition Technology in 2023", ID Tech Wire, December 2024. <https://idtechwire.com/london-police-make-540-arrests-using-live-facial-recognition-technology-in-2023/>
- 210 Katharina Buchholz, "The Most Surveilled Cities in Europe", Statista, August 2021. <https://www.statista.com/chart/19256/the-most-surveilled-cities-in-the-world/>
- 211 Solmaz Eikder, "A Battlefield Named Isfahan: Targeted Use of IMSI-Catchers and Surveillance Cameras to Enforce the Chastity and Hijab Law", Filter Watch, April, 2025. <https://filter.watch/english/2025/04/17/investigated-report-isfahan-targeted-with-imsi-catchers-and-surveillance-cameras/>
- 212 Laurent Pech, "The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU", Open Society Foundations, 2021. <https://www.opensocietyfoundations.org/uploads/c8c58ad3-fd6e-4b2d-99fa-d8864355b638/the-concept-of-chilling-effect-20210322.pdf>
- 213 "Stalkerware Grows 239% Worldwide Over the Past Three Years", Avast, March 2023. <https://press.avast.com/stalkerware-grows-239-worldwide-over-the-past-three-years>
- 214 "The Creepy Rise of Bossware", Wired, July 2023, <https://www.wired.com/story/creepy-rise-bossware/>
- 215 Valgarðsson V, Jennings W, Stoker G, et al. 2025. "A Crisis of Political Trust? Global Trends in Institutional Trust from 1958 to 2019". British Journal of Political Science. 55:e15. doi:10.1017/S0007123424000498
- 216 "Freedom in the World: The Mounting Damage of Flawed Elections and Armed Conflict", Freedom House, 2024, <https://freedomhouse.org/report/freedom-world/2024/mounting-damage-flawed-elections-and-armed-conflict>
- 217 Marina Nord, David Altman, Fabio Angiolillo, Tiago Fernandes, Ana Good God,

- and Staffan I. Lindberg. 2025. "Democracy Report 2025: 25 Years of Autocratization – Democracy Trumped?", University of Gothenburg: V-Dem Institute. https://www.v-dem.net/documents/61/v-dem-dr_2025_lowres_v2.pdf
- 218 "Report on a rule of law and human rights compliant regulation of spyware, adopted by the Venice Commission at its 141st Plenary Session", Venice Commission, Council of Europe, December 6, 2024, [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2024\)043-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2024)043-e)
- 219 French Constitutional Court Decision regarding remote activation of electronic devices in order to capture sounds and images, November 16, 2023, <https://www.conseil-constitutionnel.fr/actualites/communiqu%C3%A9/decision-n-2023-855-dc-du-16-novembre-2023-communiqu%C3%A9-de-presse>
- 220 Lee Ferran, "Nearly 100 countries have acquired cellphone spyware 'and they're using it': Official", Breaking Defense, January 16, 2025, <https://breakingdefense.com/2025/01/nearly-100-countries-have-acquired-cellphone-spyware-and-theyre-using-it-official/>
- 221 "Israeli Spyware Facilitates Human Rights Violations Globally on a Massive Scale", BDS Movement, 2021, <https://bdsmovement.net/israeli-spyware-facilitates-human-rights-violations>
- 222 Stephanie Kirchgaessner, "Critics of Putin and his allies targeted with spyware inside the EU", The Guardian, 30 May 2024, <https://www.theguardian.com/technology/article/2024/may/30/critics-of-putin-and-his-allies-targeted-with-spyware-inside-the-eu>
- 223 Vas Panagiotopoulos, "EU Commission leadership clueless about its own plan to tackle spyware crisis", Euractiv, February 19, 2025, <https://www.euractiv.com/section/politics/news/eu-commission-leadership-clueless-about-its-own-plan-to-tackle-spyware-crisis/>
- 224 Gregoire Lory and Amandine Hess, "European political landscape shifts right in 2024 as far-right gains ground", Euronews, 24 December 2024, <https://www.euronews.com/my-europe/2024/12/24/european-political-landscape-shifts-right-in-2024-as-far-right-gains-ground>
- 225 Bill Marczak, John Scott-Railton, Kate Robertson, Astrid Perry, Rebekah Brown, Bahr Abdul Razzak, Siena Anstis, and Ron Deibert, "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations", Citizen Lab, March 19, 2025 <https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/>
- 226 Angela Giuffrida and Stephanie Kirchgaessner, "Italian government approved use of spyware on members of refugee NGO, MPs told", Guardian, March 27, 2025, <https://www.theguardian.com/world/2025/mar/27/italian-government-approved-use-of-spyware-on-members-of-refugee-ngo-mps-told>
- 227 Angela Giuffrida and Stephanie Kirchgaessner, "Italian founder of migrant rescue group 'targeted with spyware'", Guardian, February 5, 2025, <https://www.theguardian.com/technology/2025/feb/05/activists-critical-of-italian-pm-may-have-had-their-phones-targeted-by-paragon-spyware-says-whatsapp>
- 228 "Casarini says will file complaint on Paragon case", ANSA, February 6, 2025, https://www.ansa.it/english/news/2025/02/06/casarini-says-will-file-complaint-on-paragon-case_824a9db9-f163-4900-a4fc-002bc28971b4.html
- 229 Vas Panagiotopoulos, "EU Commission leadership clueless about its own plan to tackle spyware crisis", Euractiv, February 19, 2025, <https://www.euractiv.com/section/tech/news/number-of-italian-spyware-victims-far-higher-than-expected-researchers-say/>
- 230 "PEGA Committee does not go all the way on spyware regulation", EDRI, May 9,

- 2025, <https://edri.org/our-work/pega-committee-does-not-go-all-the-way-on-spyware-regulation/>
- 231 Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert, "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus", Citizen Lab, July 15, 2021, <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>
- 232 Ximena Villagrán, "El CNI pagó más de 200.000 euros a Hacking Team para espiar móviles", El Confidencial, July 06, 2015, https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/
- 233 John Scott-Railton, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert, "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru", Citizen Lab, April 18, 2022, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>
- 234 Eleni Stamatoukou, "Greece Spyware Victims Refuse to Give Up After Intelligence Agency 'Exonerated'", Balkan Insight, September 24, 2024, <https://balkaninsight.com/2024/09/24/greece-spyware-victims-mull-next-steps-after-spy-agency-exonerated/>
- 235 Sarantis Michalopoulos, "Greek opposition asks if government exported 'Predator' to Sudan", Euractiv, April 17, 2023, <https://www.euractiv.com/section/politics/news/greek-opposition-asks-if-government-exported-predator-to-sudan/>
- 236 Eleni Stamatoukou, "Greece, Italy, France, 'Seeking Loopholes' for Journalists' Surveillance", BalkanInsight, December 13 2023, <https://balkaninsight.com/2023/12/13/greece-italy-and-france-are-lobbying-for-journalists-surveillance/>, Harald Schumann and Alexander Fanta, "Spying on Journalists Justified By 'National Security'", VSquare, June 19, 2023, <https://vsquare.org/spying-journalists-national-security-pegasus-predator-eu/>
- 237 Maura Forrest, "RCMP says it has not used Pegasus spyware", Politico, August 8, 2022, <https://www.politico.com/news/2022/08/08/privacy-watchdog-rcmp-spyware-00050356>
- 238 Maura Forrest, "Canada's national police force admits use of spyware to hack phones", Politico, June 29, 2022, <https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092>
- 239 "German police secretly bought Pegasus spyware", Deutsche Welle, July 7, 2021, <https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197#:~:text=According%20to%20the%20S%C3%BCddeutsche%20Zeitung%2C,since%20March%20of%20this%20year>
- 240 Kai Biermann and Holger Stark, "Die Superwaffe und die Deutschen", Zeit, July 19, 2021, <https://www.zeit.de/politik/ausland/2021-07/ueberwachungsaffaere-spionage-software-pegasus-einsatz-deutschland-bundeskriminalamt-handychdaten-rechtsstaat> [in German]
- 241 "German prosecutor opens criminal investigation into FinFisher for selling spyware to Turkey without license", ECCHR, September 5, 2019, <https://www.ecchr.eu/en/press-release/german-prosecutor-opens-criminal-investiation-into-finfisher-for-selling-spyware-to-turkey-without-license/>
- 242 "Victory! FinFisher shuts down", AccessNow, March 29, 2022, <https://www.accessnow.org/press-release/finfisher-shuts-down/>
- 243 Joe Tidy, 'Pegasus: Spyware sold to governments 'targets activists'', BBC, July 19, 2021, <https://www.bbc.com/news/technology-57881364>
- 244 Bill Marczak, John Scott-Railton, Kate Robertson, Astrid Perry, Rebekah Brown,

- Bahr Abdul Razzak, Siena Anstis, and Ron Deibert, "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations", Citizen Lab, March 19, 2025, <https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/>
- 245 Vanessa Buschschlüter, "Colombia to investigate police purchase of Pegasus spyware", BBC, September 5, 2024, <https://www.bbc.com/news/articles/ck-g5en18qvxo>
- 246 Natalie Southwick, "Surveillance Technology Is on the Rise in Latin America", Americas Quarterly, June 5, 2023, <http://americasquarterly.org/article/surveillance-technology-is-on-the-rise-in-latin-america/>
- 247 "Colombia: Freedom in the World 2025", Freedom House, <https://freedomhouse.org/country/colombia/freedom-world/2025>
- 248 Stephanie Kirchgaessner, "NSO – not government clients – operates its spyware, legal documents reveal", Guardian, November 15, 2024, <https://www.theguardian.com/technology/2024/nov/14/nso-pegasus-spyware-whatsapp>
- 249 Steven Feldstein, "When it Comes to Digital Authoritarianism, China is a Challenge — But Not the Only Challenge", War on the Rocks, February 12, 2020, <https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/>
- 250 Szabolcs Panyi, "What happened in Hungary since the Pegasus spyware revelations", Direkt36, July 18, 2023, <https://www.direkt36.hu/en/igy-hullottak-az-igazsag-morzsa-a-pegasus-ugy-ket-eve-alatt/>
- 251 Shaun Walker, "Poland launches inquiry into previous government's spyware use", Guardian, April 1, 2024, <https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use>
- 252 Jo Harper, "Polish police arrest ex-justice minister over Pegasus spyware allegations", Anadolu Ajansı, January 31, 2025, <https://www.aa.com.tr/en/europe/polish-police-arrest-ex-justice-minister-over-pegasus-spyware-allegations/3467850>
- 253 Sophie in't Veld, "An Inquiry on Spyware in the EU Revealed Abuses by Member States. Now What?", Digital Frontlines, 2023, <https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/>
- 254 Natalie Kitroeff and Ronen Bergman, "How Mexico Became the Biggest User of the World's Most Notorious Spy Tool", The New York Times, April 18, 2023, <https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html>
- 255 "Mexico: Freedom on the Net 2024", Freedom House, <https://freedomhouse.org/country/mexico/freedom-net/2024>
- 256 "Mexico: Pegasus Spyware Used on Journalists and Citizens," PEN International, March 10, 2023, <https://www.pen-international.org/news/mexico-pegasus-spyware-used-on-journalists-and-citizens>
- 257 Mexico Used Spyware on Opponents Even After It Said It Stopped," New York Times, April 18, 2023, <https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html>
- 258 "Mexico Targets Journalists, Activists with Spyware Reserved for Criminals," OCCRP, June 20, 2017, <https://www.occrp.org/en/news/mexico-targets-journalistsactivists-with-spyware-reserved-for-criminals>
- 259 ibid

- 260 "Mexico: Pegasus Spyware Used on Journalists and Citizens," PEN International, March 10, 2023, <https://www.pen-international.org/news/mexico-pegasus-spyware-used-on-journalists-and-citizens>
- 261 Suzanne Smalley, "Former Mexican president investigated over allegedly taking bribes from spyware industry", The Record, July 2025, <https://therecord.media/former-mexican-president-investigated-spyware-bribes>
- 262 Natalia Krapiva, Giulio Coppi and Rand Hammoud, "Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict", AccessNow, May 25, 2023, <https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/>
- 263 "Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict", Amnesty International, May 25, 2023, <https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/>
- 264 Miranda Patrucic and Kelly Bloss, "Life in Azerbaijan's Digital Autocracy: 'They Want to be in Control of Everything'", OCCRP, July 30, 2021, <https://www.occrp.org/en/project/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything>
- 265 Antoaneta Roussi, "Warring parties turned to spyware in Azerbaijan-Armenia conflict", Politico, May 25, 2023, <https://www.politico.eu/article/warring-parties-spyware-azerbaijan-armenia-conflict-pegasus-hacking/>
- 266 "Pegasus Project: Leaked database includes 300 Indian phone numbers", Financial Express, July 19, 2021, <https://www.financialexpress.com/life/technology-pegasus-project-leaked-database-includes-300-indian-phone-numbers-2292937/>
- 267 Anandita Mishra and Tanmay Singh, "Pegasus Investigation Report to remain in sealed cover despite containing evidence that 5 phones had malware", Internet Freedom Foundation, August 26, 2022, <https://shorturl.at/pbmju>
- 268 Boris Pradhan, "Nothing wrong in country using spyware": Supreme Court on Pegasus row", Business Standard, April 29, 2025, https://www.business-standard.com/india-news/supreme-court-says-technical-report-on-pegasus-will-not-be-made-public-125042900434_1.html
- 269 John Scott-Railton, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert, and Ron Deibert, "GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement", Citizen Lab, July 17, 2022, <https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/>
- 270 "Pegasus Spyware: A Grave Threat to Journalists in Southeast Asia", Aljazeera Media Institute, February 5, 2024, <https://institute.aljazeera.net/en/ajr/article/2525>
- 271 "Global: A Web of Surveillance – Unravelling a murky network of spyware exports to Indonesia", Amnesty International, May 2, 2024, <https://www.amnesty.org/en/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/>
- 272 "Israeli firms sold invasive surveillance tech to Indonesia: Report", Aljazeera, May 3, 2024, <https://www.aljazeera.com/news/2024/5/3/israeli-firms-sold-invasive-surveillance-tech-to-indonesia-report>
- 273 "Spyware attack attempts on mobile devices of members of civil society discovered", SHARE Foundation, November 20 2023, <https://sharefoundation.info/en/spyware-attack-attempts-on-mobile-devices-of-members-of-civil-society-discovered/>

- 274 “BIRN Serbia journalists targeted with spyware”, SHARE Foundation, March 28 2025, <https://sharefoundation.info/en/birn-serbia-journalists-targeted-with-spyware/>
- 275 ““A Digital Prison”: Surveillance and the suppression of civil society in Serbia”, Amnesty International, December 16 2024, <https://www.amnesty.org/en/documents/eur70/8813/2024/en/>
- 276 “Cellebrite zero day exploit used to target phone of Serbian student activist”, Amnesty International, February 28 2025, <https://www.amnesty.org/en/documents/eur70/9118/2025/en/>
- 277 Cooper Quintin, Rebekah Brown, and John Scott-Railton, “Something to Remember Us By Device Confiscated by Russian Authorities Returned with Monokle-Type Spyware Installed”, Citizen Lab, December 5 2024, <https://citizenlab.ca/2024/12/device-confiscated-by-russian-authorities-returned-with-monokle-type-spyware-installed/>
- 278 Kevin Poireault, “Lookout Discovers New Spyware Deployed by Russia and China”, Infosecurity Magazine, December 2024, <https://www.infosecurity-magazine.com/news/lookout-new-spyware-russia-china/>
- 279 “Lookout Discovers New Chinese Surveillance Tool Used by Public Security Bureaus”, Lookout, December 2024, <https://www.lookout.com/threat-intelligence/article/eaglemsgspy-chinese-android-surveillanceware>
- 280 Andrei Soldatov, “Why Is Russia Not Using Pegasus Spyware?”, The Moscow Times, July 21, 2021, <https://www.themoscowtimes.com/2021/07/21/why-is-russia-not-using-pegasus-spyware-a74572>
- 281 Maya Wang, “China’s Dystopian Push to Revolutionize Surveillance”, Human Rights Watch, August 18, 2017, <https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance#:~:text=the%C2%A0Gold-en%20Shield%20Project%20in%C2%A02000,the%20push%20of%20a%20button>
- 282 Bill Toulas, “Russia to enforce location tracking app on all foreigners in Moscow”, Bleeping Computer, May 2025, <https://www.bleepingcomputer.com/news/government/russia-to-enforce-location-tracking-app-on-all-foreigners-in-moscow/>
- 283 Cooper Quintin, Rebekah Brown, and John Scott-Railton, “Something to Remember Us By Device Confiscated by Russian Authorities Returned with Monokle-Type Spyware Installed”, Citizen Lab, December 5 2024, <https://citizenlab.ca/2024/12/device-confiscated-by-russian-authorities-returned-with-monokle-type-spyware-installed/>
- 284 Kevin Poireault, “Lookout Discovers New Spyware Deployed by Russia and China”, Infosecurity Magazine, December 2024, <https://www.infosecurity-magazine.com/news/lookout-new-spyware-russia-china/>
- 285 “US says disabled Russian spyware used for two decades”, France24, May 9, 2023, <https://www.france24.com/en/live-news/20230509-us-says-disabled-russian-spyware-used-for-two-decades>
- 286 Jonathan Greig, “Chinese provincial security teams used spyware to collect texts, audio recordings”, The Record, December 11, 2024, <https://therecord.media/chinese-provincial-security-teams-use-spyware-collect-texts-location>
- 287 “Lookout Discovers New Chinese Surveillance Tool Used by Public Security Bureaus”, Lookout, December 2024, <https://www.lookout.com/threat-intelligence/article/eaglemsgspy-chinese-android-surveillanceware>
- 288 Matthew Humphries, “China Is Installing Spyware on Tourists’ Phones”, PCMag,

- July 3, 2019 <https://www.pcmag.com/news/china-is-installing-spyware-on-tourists-phones>
- 289 Kevin Poireault, "China-Backed Hackers Exploit BRICKSTORM Backdoor to Spy on European Businesses", Infosecurity Magazine, April 16, 2025, <https://www.infosecurity-magazine.com/news/china-hackers-brickstorm-backdoor/>
- 290 Sam Sabin, "Sensitive phone data flows through China", Axios, April 22, 2025, <https://www.axios.com/2025/04/22/sensitive-phone-data-flows-through-china-future-of-cybersecurity>
- 291 Ofir Rozmann, Asli Koksall and Sarah Bock, "I Spy With My Little Eye: Uncovering an Iranian Counterintelligence Operation", Google Cloud, August 24, 2024, <https://cloud.google.com/blog/topics/threat-intelligence/uncovering-iranian-counterintelligence-operation>
- 292 "Bahrain loses bid to block dissidents' spyware lawsuit in UK", Reuters, October 4, 2024, <https://www.reuters.com/world/bahrain-loses-state-immunity-appeal-dissidents-uk-lawsuit-over-spyware-2024-10-04/>
- 293 "Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence", Amnesty International, March 9, 2022, <https://www.amnesty.org/en/latest/news/2022/03/morocco-western-sahara-activist-nso-pegasus/>
- 294 Zach Campbell and Lorenzo D'Agostino, "How the EU supplied Morocco with phone-hacking spyware", Disclose, July 25, 2022, <https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware>
- 295 Laura Hülsemann, "Spanish court halts probe into Israeli spyware hacking of Pedro Sánchez's phone", Politico, July 10, 2023, <https://www.politico.eu/article/spain-shutters-investigation-into-pegasus-hacking-of-pedro-sanchez-phone/>
- 296 "Iran uses spyware to track and control citizens' phones at protests – leaked documents", Middle East Monitor, November 3, 2024, <https://web.archive.org/web/20250426110954/https://www.middleeastmonitor.com/20221103-iran-uses-spyware-to-track-and-control-citizens-phones-at-protests-leaked-documents/>
- 297 Sam Biddle and Murtaza Hussain, "The documents provide an inside look at an Iranian government program that lets authorities monitor and manipulate people's phones", The Intercept, October 28 2022, <https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/>
- 298 Nima Khorrami, "Navigating Cybersecurity and Surveillance: Iran's Dual Strategy for National Security", Washington Institute, May 29, 2024, <https://www.washingtoninstitute.org/policy-analysis/navigating-cybersecurity-and-surveillance-irans-dual-strategy-national-security#:~:text=What%27s%20particularly%20noteworthy%20is%20that,to%20monitor%20political%20activists%2C%20dissidents>
- 299 Stephanie Kirchgaessner, "US announces new restrictions to curb global spyware industry", Guardian, February 5, 2024, [https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions; Stephanie Kirchgaessner, "Israeli spyware company NSO Group placed on US blacklist", Guardian, November 3, 2021, <https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist>](https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions; Stephanie Kirchgaessner, 'Israeli spyware company NSO Group placed on US blacklist', Guardian, November 3, 2021, https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist)
- 300 "Germany charges executives for selling spyware to Turkey", Deutsche Welle, May 22, 2023, <https://www.dw.com/en/germany-charges-executives-for-selling-spyware-to-turkey/a-65701848>
- 301 "Global Surveillance", Privacy International, https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

- 302 Steven Feldstein and Brian (Chun Hey) Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses", Carnegie Endowment for International Peace, March 14, 2023, <https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en>
- 303 "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations", Citizen Lab, 19 March 2025, <https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/>
- 304 <https://techcrunch.com/2025/02/04/spyware-maker-paragon-confirms-u-s-government-is-a-customer/>
- 305 "Deadly Exchange: The Dangerous Consequences of American Law Enforcement Trainings in Israel", Researching the American-Israeli Alliance (RAIA) and Jewish Voice for Peace, September 2018, <https://deadlyexchange.org/wp-content/uploads/2019/07/Deadly-Exchange-Report.pdf>
- 306 Connor Woodman, "Chickens Come Home to Roost: the U.S. Empire, the Surveillance State and the Imperial Boomerang", Verso Books, June 10, 2020, <https://www.versobooks.com/en-gb/blogs/news/4417-chickens-come-home-to-roost-the-u-s-empire-the-surveillance-state-and-the-imperial-boomerang>
- 307 Henrik Moltke, "Mission Creep: How the NSA's Game-Changing Targeting System Built for Iraq and Afghanistan Ended Up on the Mexico Border", The Intercept, May 29, 2019, <https://theintercept.com/2019/05/29/nsa-data-afghanistan-iraq-mexico-border/>
- 308 Yossi Melman, "Israel's Spyware Diplomacy Is an Extension of Its Long Bloody History of Arms Sales", Haaretz, February 2, 2022, <https://www.haaretz.com/israel-news/tech-news/2022-02-03/ty-article/premium/israels-spyware-diplomacy-is-an-extension-of-its-long-bloody-history-of-arms-sales/0000017f-f882-ddde-abff-fce787ac0000>
- 309 "Israeli Cyber Annual Insights and 2025 Trends", Startup Nation Central, March 9, 2025, <https://startupnationcentral.org/hub/blog/israeli-cyber-annual-insights-and-2025-trends/>
- 310 Frankie Vetch, "Israel uses Palestine as a petri dish to test spyware", Coda Story, June 22, 2023, <https://www.codastory.com/authoritarian-tech/israel-spyware-palestine-antony-loewenstein/>
- 311 Elianne Shewring, "Israel's Spyware Law: A Step Towards Authoritarianism?", GIGA Focus Middle East, 2025(1), Hamburg: German Institute for Global and Area Studies (GIGA), <https://doi.org/10.57671/gfme-25012>
- 312 Yossi Melman, "Israel's Immoral Arms Export Must End", Haaretz, August 2, 2021, <https://www.haaretz.com/opinion/2021-08-02/ty-article/premium/israels-immoral-arms-export-must-end/0000017f-dbd7-d856-a37f-ffd70ad30000>
- 313 Steven Feldstein and Brian Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses", Carnegie Endowment for International Peace, March 2023, <https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en>
- 314 Jen Roberts et al, "Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights", Atlantic council, September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/>

- 315 Lorenzo Franceschi-Bicchierai, "How Barcelona became an unlikely hub for spyware startups", TechCrunch, January 13, 2025, <https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/>
- 316 Jen Roberts et al, "Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights", Atlantic council, September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/>
- 317 Justin Albrecht and Paul Shunk, "Lookout Uncovers Hermit Spyware Deployed in Kazakhstan", Lookout, June 2022, <https://www.lookout.com/threat-intelligence/article/hermit-spyware-discovery>
- 318 Alex Hern, "Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim", The Guardian, Jul 2015, <https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim>
- 319 Lorenzo Franceschi-Bicchierai, "Hacking Team Founder: Hacking Team is Dead", Vice, May 2020, <https://www.vice.com/en/article/hacking-team-is-dead/>
- 320 Gianmarco Daniele, "Modern mafia: Italy's organised crime machine has changed beyond recognition in 30 years", The Conversation, January 2023, <https://theconversation.com/modern-mafia-italys-organised-crime-machine-has-changed-beyond-recognition-in-30-years-198352>
- 321 Suzanne Smalley, "How Italy became an unexpected spyware hub", The Record, November 2024, <https://therecord.media/how-italy-became-an-unexpected-spyware-hub>
- 322 "Surveillance software "made in Germany" for Turkish authorities? Public Prosecutor's Office charges FinFisher executives", ECCHR, <https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfother/>
- 323 Vikki Davies, "Who are NSO Group, the company being sued by Apple?", Cyber Magazine, November 2021, <https://cybermagazine.com/cyber-security/who-are-nso-group-company-being-sued-apple>
- 324 "Fact Sheet: the Israeli Cyber Industry", Medium, August 2022, <https://visualizingpalestine.medium.com/fact-sheet-the-israeli-cyber-industry-d2a64b43094>
- 325 Ibid.
- 326 Anthony Loewenstein, "How Palestine Became Israel's Spyware Test-Bed", New Internationalist, October 2023, <https://newint.org/features/2023/10/02/spy-games>
- 327 Yossi Melman, "Israel's Spyware Diplomacy Is an Extension of Its Long Bloody History of Arms Sales", Haaretz, February 2, 2022, <https://www.haaretz.com/israel-news/tech-news/2022-02-03/ty-article/premium/israels-spyware-diplomacy-is-an-extension-of-its-long-bloody-history-of-arms-sales/0000017f-f882-ddde-abff-fce787ac0000>
- 328 Hope O'Dell, "How the US has used its power in the UN to support Israel for decades", The Chicago Council on Global Affairs, December 18, 2023, <https://globalaffairs.org/commentary-and-analysis/blogs/how-us-has-used-its-power-un-support-israel-decades>
- 329 "Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware", European Parliament, May 2023, <https://www.>

- europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html
- 330 Lorenzo Franceschi-Bicchierai, "Price of zero-day exploits rises as companies harden products against hackers", TechCrunch, April 2024, <https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/>
- 331 Ibid.
- 332 Casey Charrier, James Sadowski, Clement Lecigne, Vlad Stolyarov, "Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis", Google Threat Intelligence Group, April 2025, <https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends>
- 333 Lorenzo Franceschi-Bicchierai, "Price of zero-day exploits rises as companies harden products against hackers", TechCrunch, April 2024, <https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/>
- 334 Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani and Michael Safi, "The Pegasus Project", The Guardian, Jul 2021, <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>
- 335 "Pegasus: The cost of spying with one of the most powerful spyware in the world", Freemindtronic, October 2023, <https://freemindtronic.com/pegasus-the-cost-of-spying-with-one-of-the-most-powerful-spyware-in-the-world/>
- 336 "Greece's Surveillance Scandal Must Shake Us Out of Complacency", Amnesty International, January 2023, <https://www.amnesty.org/en/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/>
- 337 "The Predator Files: Caught in the Net. The Global Threat from "EU Regulated" Spyware", Amnesty International, October 2023, <https://www.amnesty.org/en/documents/act10/7245/2023/en/>
- 338 Shuki Sadeh, "A Shady Israeli Intel Genius, His Cyber-spy Van and Million-dollar Deals", Haaretz, December 2020, <https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000>
- 339 David Kenner and Eve Sampson, "Spyware firm Intellexa hit with US sanctions after Cyprus Confidential expose", International Consortium of Investigative Journalists, March 2024, <https://www.icij.org/investigations/cyprus-confidential/spyware-firm-intellexa-hit-with-us-sanctions-after-cyprus-confidential-expose/>
- 340 Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Aljizawi, Siena Anstis, Kristin Berdan, and Ron Deibert, "Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytox Mercenary Spyware", December 2021, <https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/>
- 341 Thomas Brewster, "Meet Paragon: An American Funded, Super-Secretive Israeli Surveillance Startup That 'Hacks WhatsApp And Signal", Forbes, Jul 2021, <https://www.forbes.com/sites/thomasbrewster/2021/07/29/paragon-is-an-nso-competitor-and-an-american-funded-israeli-surveillance-startup-that-hacks-encrypted-apps-like-whatsapp-and-signal/>
- 342 Bill Marczak, John Scott-Railton, Kate Robertson, Astrid Perry, Rebekah Brown, Bahr Abdul Razzak, Siena Anstis, and Ron Deibert, "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations", Citizen Lab, March 2025,

- <https://www.forbes.com/sites/thomasbrewster/2021/07/29/paragon-is-an-nso-competitor-and-an-american-funded-israeli-surveillance-startup-that-hacks-encrypted-apps-like-whatsapp-and-signal/>
- 343 “Netanyahu’s cabinet pushes for changes to cyber export rules”, Intelligence Online, January 2023, <https://www.intelligenceonline.com/government-intelligence/2023/01/16/netanyahu-s-cabinet-pushes-for-changes-to-cyber-export-rules.109902045-art>
 - 344 Siena Anstis, “Litigation and other formal complaints related to mercenary spyware”, The Citizen Lab, December 2018, <https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/>
 - 345 “The Beckham Tax Law Explained: Understanding Spain’s Expat Tax Benefits”, Marfour International Law, <https://marfourlaw.com/beckham-tax-law/>
 - 346 Lorenzo Franceschi-Bicchierai, “How Barcelona Became an Unlikely Hub for Spyware Startups”, TechCrunch, January 2025, <https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/>
 - 347 Jen Roberts et al, “Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights”, Atlantic council, September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/>
 - 348 Steven Feldstein and Brian (Chun Hey) Kot, “Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses”, Carnegie Endowment for International Peace, March 14, 2023, <https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/> <https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en>
 - 349 “What is Stalkerware? How to Find and Remove Stalkerware”, Kaspersky, <https://www.kaspersky.com/resource-center/definitions/what-is-stalkerware>
 - 350 “FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women”, UNWomen, February 10, 2025, <https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women>
 - 351 Neil Mitchell, “Millennial parents driving a change in online safety and digital parenting”, Verizon, January 2021, <https://www.verizon.com/about/parenting/millennial-parents-driving-change-digital-parenting>
 - 352 Emma McGowan, “Stalkerware won’t keep your kids safe”, Avast, February 2021, <https://blog.avast.com/stalkerware-and-children-avast>
 - 353 Chatterjee, Rahul; Doerfler, Periwinkle; Orgad, Hadas et al. The Spyware Used in Intimate Partner Violence, in Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP 2018) (San Francisco: Institute of Electrical and Electronics Engineers, 2018), 441–458, <https://doi.org/10.1109/SP.2018.00061>
 - 354 “The State of Stalkerware in 2023”, Kaspersky, February 2024, <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/03/07160820/The-State-of-Stalkerware-in-2023.pdf>
 - 355 Lorenzo Franceschi-Bicchierai, “Hacked, leaked, exposed: Why you should never use stalkerware apps”, TechCrunch, March 19, 2025, <https://techcrunch.com/2025/03/19/hacked-leaked-exposed-why-you-should-stop-using-stalkerware-apps/>

- 356 Zack Whittaker, "Data breach exposes millions of mSpy spyware customers", TechCrunch, July 11, 2024, <https://techcrunch.com/2024/07/11/mspy-spyware-millions-customers-data-breach/>
- 357 Zack Whittaker, "Behind the stalkerware network spilling the private phone data of hundreds of thousands", TechCrunch, February 2022, <https://techcrunch.com/2022/02/22/stalkerware-network-spilling-data/>
- 358 Coalition Against Stalkerware, <https://stopstalkerware.org/>
- 359 Bill Budington, "Stalkerware Maker Fined \$410k and Compelled to Notify Victims", Electronic Frontier Foundation, February 2023, <https://www.eff.org/deeplinks/2023/02/stalkerware-maker-fined-410k-and-compelled-notify-victims>
- 360 Ibid.
- 361 "The State of Stalkerware in 2023", Kaspersky, February 2024, <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/03/07160820/The-State-of-Stalkerware-in-2023.pdf>
- 362 Zoë Corbyn, "'Bossware is coming for almost every worker': the software you might not realize is watching you", The Guardian, 27 April 2022, <https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic>
- 363 Bennett Cyphers and Karen Gullo, "Inside the Invasive, Secretive 'Bossware' Tracking Workers", Electronic Frontier Foundation, June 2020, <https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers>
- 364 Ibid.
- 365 "Bossware and Employment Tech Database", Coworker, November 2021, <https://home.coworker.org/worktech/>
- 366 Luke Munn, "Expansive and Invasive: Mapping 'Bossware' Used to Monitor Workers", Surveillance and Society 22(2): 104-119, 2024, <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/16179>
- 367 Megan Carnegie, "The Creepy Rise of Bossware", Wired, July 2023, <https://www.wired.com/story/creepy-rise-bossware/>
- 368 Luke Munn, "Expansive and Invasive: Mapping 'Bossware' Used to Monitor Workers", Surveillance and Society 22(2): 104-119, 2024, <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/16179>
- 369 Ibid.
- 370 Andrew Manley and Shaun Williams, "We're Not Run on Numbers, We're People, We're Emotional People": Exploring the Experiences and Lived Consequences of Emerging Technologies, Organizational Surveillance and Control among Elite Professionals", Organization 29 (4): 692–713, Jul 2022, <https://research-portal.bath.ac.uk/en/publications/were-not-run-on-numbers-were-people-were-emotional-people-explori>
- 371 Naomi Klein, "The Shock Doctrine: The Rise of Disaster Capitalism", Macmillan, 2007.

PHOTO CREDIT

Photo by [Scott Rodgerson on Unsplash](#)
 Photo by [Henrique Dias on Unsplash](#)
 Photo by [Domagoj on Unsplash](#)
 Photo by [Vadim Sadovski on Unsplash](#)
 Photo by [Andrea Leopardi on Unsplash](#)
 Photo by [Parker Hilton on Unsplash](#)
 Photo by [Vishwanth Pindiboina on Unsplash](#)
 Photo by [prasetyo irawan on Unsplash](#)
 Photo by [Kromwell Lopez on Unsplash](#)
 Photo by [Vera Gorbunova on Unsplash](#)
 Photo by [Jezael Melgoza on Unsplash](#)
 Photo by [Arun kuttiyani on Unsplash](#)
 Photo by [Anton Lukin on Unsplash](#)
 Photo by [Jorge Fernández Salas on Unsplash](#)
 Photo by [Anna Berdnik on Unsplash](#)
 Photo by [Pham Trong Ho on Unsplash](#)
 Photo by [Museums Victoria on Unsplash](#)
 Photo by [Jason Dent on Unsplash](#)
 Photo by [NighthawStudio on Unsplash](#)
 Photo by [Kaspars Eglitis on Unsplash](#)
 Photo by [Martin Baron on Unsplash](#)
 Photo by [gavriiloandric on Protest.pics](#)
 Photo by [John Angel on Unsplash](#)
 Photo by [David Lee on Unsplash](#)
 Photo by [Hale Tat on Unsplash](#)
 Photo by [Cong Wang on Unsplash](#)
 Photo by [Oansen on Unsplash](#)
 Photo by [kate.sade on Unsplash](#)

