Spyware and state abuse

THE CASE FOR AN EU-WIDE BAN

EDRi
European Digital Rights

TABLE OF CONTENTS

This position paper was coordinated by **Aljosa Ajanovic, EDRi Policy Advisor.**

We would like to express our sincere gratitude to the whole EDRi network, upon whose work this report builds. In particular, we would like to thank the following people for making a particular contribution to this report:

→ Chloé Berthélémy, EDRi
→ Jesper Lund, IT-Pol Denmark
→ Bastien Le Querrec, La Quadrature du Net
→ Andrijana Ristic, SHARE Foundation
→ Rand Hammoud, Access Now
→ Luzie Neyenhuys, Society for Civil Rights (Gesellschaft für Freiheitsrechte)
→ Hannah Lichtenthäler, SUPERRR Lab
→ Rejo Zenger, Bits of Freedom
→ Michaela Nakyama Shapiro, Article 19
→ Walter van Holst, Vrijschrift.org

ABSTRACT

The use of spyware has become one of the **most pressing threats to democracy, fundamental rights, and cybersecurity** in the European Union and globally. Both state and private actors have engaged in the widespread deployment of commercial spyware, often with devastating consequences for individuals' privacy, political freedoms, and personal safety. The spyware industry has flourished under a system of permissiveness, legal loopholes, and weak regulatory oversight, **turning Europe into a hub for the development, trade, use and export of these harmful technologies.**

Spyware operates through exploiting vulnerabilities, compromising device integrity, and enabling remote, often undetectable, access to vast amounts of personal data. **Its use, whether by state security services, private companies, or individuals, fundamentally violates the principles of necessity and proportionality under European human rights law.** The commercial spyware market not only enables unlawful state surveillance but also fuels gender-based violence, coercive control, and destabilisation of entire communities.

The proliferation of spyware **has been enabled by the EU's own internal market rules,** the absence of uniform regulation, and **a thriving commercial vulnerabilities market.** States and private vendors have profited from this "intrusion-as-a-service" model, while **victims face enormous obstacles to obtaining redress.** The EU's failure to regulate this industry has global consequences, encouraging its expansion into candidate countries and beyond, further eroding democratic norms and security worldwide.

Given the inherent risks of spyware and the structural nature of these abuses, **we conclude that no meaningful safeguards can make the use of spyware compatible with fundamental rights.** Therefore, **EDRi calls 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. Only a total ban can effectively protect human rights, close regulatory gaps, and end the EU's role in the global proliferation of spyware.

In addition, the EU must take urgent steps to address the broader spyware ecosystem:

→ **End the commercial spyware market** by prohibiting the operation of spyware vendors and investors and the export of spyware from within the EU. This business model based on secrecy, vulnerabilities, and abuse must be dismantled to prevent further expansion of this industry.

→ **End the vulnerabilities and exploit market** by banning the commercial trade of vulnerabilities for this purposes. Public funding and procurement must no longer fuel the development of new exploits. Resources should instead be redirected toward coordinated vulnerability disclosure, good-faith researchers and cybersecurity strengthening

→ **Ensure access to remedies for victims** that have already suffered spyware abuse, by creating clear legal avenues for individuals to seek redress, including judicial remedies, reparation mechanisms, and state accountability for unlawful spyware use. The EU must also ensure effective investigation, prosecution, and sanctions against perpetrators and investors, including political and administrative accountability for public officials responsible for spyware abuses.

1. INTRODUCTION

The term 'spyware' has increasingly entered the political and public lexicon after a series of scandals that, across the world, have unfolded due to the use of spyware tools by many state authorities for unlawful surveillance. Alongside the use of government-developed spyware in countries like Germany and Serbia, it is reported that at least 14 European Union (EU) countries have used to commercial spyware.[1] Although the reported use varies in intensity,[2] it reveals a worrisome reality: the acquisition and deployment of commercial spyware tools have become widespread, and regulation remains almost entirely absent.

The unregulated expansion of the commercial spyware market has enabled governments to access such tools with ease, despite their capacity to disproportionately limit people's rights and cause serious harm. The situation is particularly concerning as spyware poses severe threats to the protection of fundamental rights, democratic stability and collective safety. As spyware implies a particularly serious interference with the rights to privacy and data protection guaranteed by the Charter of Fundamental Rights of the EU, it also affects the exercise of other rights and freedoms, such as freedom of expression, association and assembly.

Civil society organisations and media outlets have repeatedly documented the use of spyware against journalists, activists, opposition figures and human rights defenders. In a wider context of shrinking civic space in Europe, this contributes to a chilling effect and therefore, **constitutes** a serious threat to European democratic rule-of-law systems. Furthermore, the targeting of high-ranking officials, such as the Prime Minister of Spain[3] or the President of France,[4] also raises issues of states' essential security interests and potential democratic interference.

The proliferation of commercial spyware systems such as Pegasus,[5] Predator,[6] Candiru[7] or Graphite[8] has highlighted the urgent need for comprehensive action at the European Union (EU) level. Despite growing evidence of systematic abuse, legislative responses have been slow and inadequate, allowing commercial spyware vendors to profit significantly from these human rights violations.[9]

The EU's permissiveness towards the commercial spyware market and Member States' unchecked use affects not only the EU itself but also other regions. For example, this situation creates a legitimacy and a blueprint for the production and use of such tools in its areas of influence, such as candidate countries like Serbia, North Macedonia and other Western Balkan countries, as well as by other partners with close ties to the EU. **Furthermore, by being established in the EU, private vendors gain marketing legitimacy to sell their products to non-EU states.**

1. *Atlantic Council,* "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights," September 4, 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/.*
2. From more than 500 people spied on in Poland, Associated Press, "Poland Says Pegasus Spyware Was Used to Hack Over 500 Phones," December 21, 2023, *https://apnews.com/article/poland-spyware-pegasus-nso-group-israel-413bb3cb27daac011d52b524c6d16160,* to the news that the Slovak government had simply acquired Pegasus, European Parliament, "Answer to Parliamentary Question: E-001920/2024," April 12, 2024, *https://www.europarl.europa.eu/doceo/document/E-10-2024-001920_EN.html*
3. *Politico,* "Spanish PM Pedro Sánchez Had Phone Hacked with Pegasus Spyware," May 2, 2022, *https://www.politico.eu/article/pegasus-spyware-targeted-spanish-pm-pedro-sanchez-defense-minister/*
4. *Le Monde,* "Projet Pegasus : un téléphone portable d'Emmanuel Macron dans le viseur du Maroc," july 20, 2021, *https://www.lemonde.fr/projet-pegasus/article/2021/07/20/projet-pegasus-un-telephone-portable-d-emmanuel-macron-dans-le-viseur-du-maroc_6088950_6088648.html*
5. *Amnesty International,* "Forensic Methodology Report: How to Catch NSO Group's Pegasus," July 18, 2021, *https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/*
6. *Sekoia.io,* "Predator Spyware," accessed May 20, 2025, *https://www.sekoia.io/en/glossary/predator-spyware/*
7. *Citizen Lab,* "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," July 15, 2021, *https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/*
8. *Citizen Lab,* "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations," March 19, 2025, *https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/*
9. According to the Carnegie Endowment for International Peace, the global sale of spyware reached over 12 billion dollars in 2023 (Carnegie Endowment for International Peace, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," March 14, 2023, *https://carnegieendowment.org/research/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses*

This paper aims to address the specific challenges posed by spyware use and its commercial proliferation. It builds on and complements EDRi's 2022 position paper, State Access to Encrypted Data – A Digital Rights Perspective,[10] which examined various forms of state hacking, including mandated encryption backdoors and compelled access to devices. In that paper, **EDRi** assessed important developments in EU legislation, policy debates and police operations from a fundamental rights perspective and as a result, **found the use of spyware incompatible with standards of a democratic society based on the rule of law.**[11]

At the time of writing this paper, the European Commission and **EU Member States are attempting once again to address** the false problem of 'Going Dark'[12] via multiple (non-) legislative initiatives in order to grant law enforcement maximal access to personal data.[13] In this context, we have observed two narrative trends. The first calls for the use of spyware as a purportedly "more proportionate" and thus desirable means of surveillance because of its allegedly "targeted" use. According to this logic, spyware is compared to other potential forms of hacking, such as mandated encryption backdoors, which are considered less convenient by comparison because they require the systematic weakening of encryption and other digital security systems at the design stage of all devices or communication services.

The second trend uses the opposite argument: supporting encryption backdoors as the least privacy-intrusive solution for targeted access, mainly because of the regulatory context in which they sit. From that viewpoint, (commercial) spyware is portrayed as uncontrollable, a tool that cannot be regulated due to its production by foreign private actors like Israeli spyware companies.

However, we refute this false dichotomy. Whether through backdoors or spyware, **both claims rely on the same underlying principle. Both'solutions' require the exploitation (and even creation) of technical vulnerabilities which undermine the integrity of digital systems and thus the security of all users.** With that in mind, the use of spyware or encryption backdoors **cannot meet the claims that these measures are targeted. Therefore these two techniques are equally dispropotionate, as they both pose profound threats to a range of fundamental rights and to our collective digital security.**

A tacit assumption underlying the 'Going Dark' debate is that no communication or data must be beyond the effective reach of law enforcement or intelligence services, which is incorrect. First, the state has never had omniscient capacities and thus, the claim that law enforcement authorities are currently falling behind like never before because of modern means of communication is simply inaccurate from a historical perspective. Second, EU primary law grants the possibility to restrict fundamental rights, such as the right to private life by accessing private communications, only under very specific circumstances. It does not mean that all means are justified to enable such restriction – quite the contrary. This is a key concept of European human rights law: the ends do not always justify the means, and the coercive power of the state must be circumscribed. Therefore, **there are cases in which law enforcement may not or cannot access communications. That is a *sine qua non* condition for a democratic and free society which protects people's rights and autonomy from government overreach.**

EDRi's call for the prohibition of the development, production, marketing, acquisition, sale, import, export, and use of spyware in EU Member States requires a clarification of the definition of what constitutes spyware. Furthermore, we believe that the growth of the spyware industry, the exponential rise in scandals of spyware use by states, and the impact of spyware on human rights and democracy have been such that they now require a more focused analysis **from a holistic human rights viewpoint**. In the last few years, the commercial spyware market has expanded rapidly with the proliferation of spyware vendors[14] and a lucrative vulnerabilities market, in which private actors exploit software flaws to illegally infiltrate devices.

First, this paper attempts to clarify the **definition of spyware,** as the lack of a precise, enforceable definition has so far hindered efforts to regulate its use. **We advocate for spyware to be prohibited, and this ban must have a clear scope, defining spyware as any software that, mainly through vulnerabilities, covertly infiltrates a device, compromising its integrity and enabling remote monitoring, data gathering, data extraction, control, and/or manipulation.**

Second, this paper analyses **the role and growth of the commercial spyware market,** arguing that it poses an **inherent threat to our collective security, democracy, and human rights, and thus should be prohibited.**

Third, we examine the possibilities of **remedies for victims of state use of spyware,** advocating for a comprehensive list of measures to offer reparation to all victims, across Europe and beyond, who so far have been denied justice and neglected by authorities.

10. *EDRi*, "State access to encrypted data, A digital rights perspective", October 2022, *https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf*
11. idem
12. 'Going Dark' is a term used "to describe [the] decreasing ability [of law enforcement agencies] to lawfully access and examine evidence at rest on devices and evidence in motion across communications networks" due in large parts to the increasing use of encryption. IACP, 2015 "Summit Report. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence", *https://www.theiacp.org/sites/default/files/2019-05/IACPSummitReportGoingDark_0.pdf*
13. *EDRi*, High-Level Group "Going Dark" outcome: A mission failure, June 13, 2024, *https://edri.org/our-work/high-level-group-going-dark-outcome-a-mission-failure/*
14. See 'Commercial spyware vendors' in the Glossary

2. WHAT IS SPYWARE? A LASTING DEFINITION

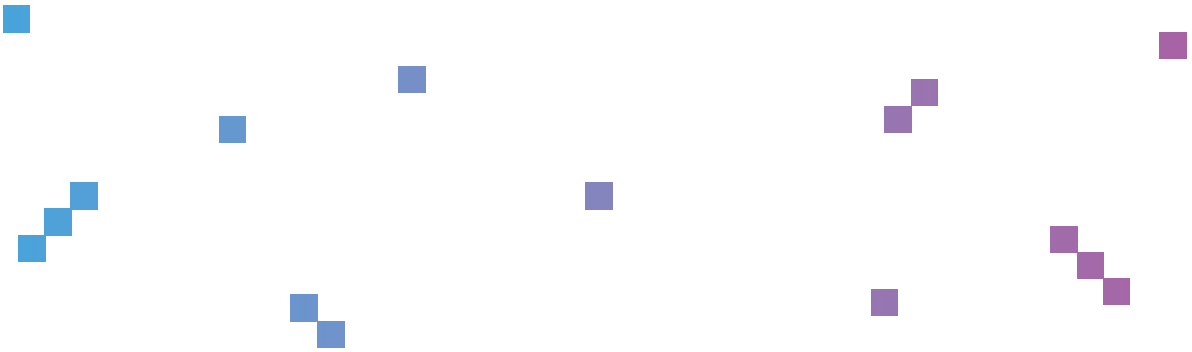
This section aims to define spyware. It addresses hacking tools used by states for surveillance but also other types, such as stalkerware and forensic tools, in order to clarify the scope of this paper and of any regulatory framework concerning spyware.

2.1 Defining 'spyware': a holistic and sustainable approach

2.1.1 A definition that anticipates future threats

When hearing the word 'spyware', Pegasus, developed by the notorious Israeli company NSO Group - may comes to mind, along with similar programs that have made headlines **in recent years.** However, many other software tools with different capabilities also fall under the category of spyware. Emerging technological developments, such as AdInt[15] - which can infect devices via seemingly innocuous targeted ads - illustrate how quickly restrictive or detailed definitions become outdated.

The **commercial spyware industry** continues to evolve, often exploiting legal loopholes, and developing specific technologies in an attempt to avoid traditional classification. Therefore, a **sustainable definition of *spyware* that is enforceable and resilient must focus on *what spyware does*, rather than how it is marketed or who uses it. It must also be broad in scope** to ensure that any software with the described capabilities is captured under the regulatory framework, thus **preventing future harm.** Otherwise, limiting the definition to only the most invasive types would leave many privacy-violating tools outside the scope of the law, creating a legal vacuum that can be exploited by both states and malicious actors.



15. AdInt refers to a new type of practices, "Ad intelligence", which are techniques that turn data collected for advertising purposes into intelligence. It has been reported that Israeli companies are developing software that can infect a device through seemingly inoffensive targeted ads. Intelligence Online "Offensive AdInt Is Israeli Cyber Sector's New Secret Weapon", February 15, 2024. *https://www.intelligenceonline.com/surveillance--interception/2024/02/15/offensive-adint-is-israeli-cyber-sector-s-new-secret-weapon,110159842-eve*

2.1.2 Core characteristics: which type of software qualifies as spyware?

When seeking to draw the scope of a ban on spyware use, it is necessary to attempt to describe the techniques and tools that we aim to prohibit. From our observation of current and past hacking tools, spyware can be defined as any **software** that meets the following **cumulative conditions:**

1. It is **installed or run on a device without the free and informed consent of the user;**

2. **It compromises the integrity** of the device: meaning that the software modifies, temporarily or permanently, one or more elements of the device, including, among others, the volatile memory (RAM)1 and other internal memories, internal chips or storage drives. This element differentiates spyware from some of the traditional forensic tools, which theoretically limit themselves to data extraction and do not alter the device or any stored information on it in a way that is not detectable by authorised users, unlike forensic tools (see section below). This device integrity principle is key to the requirements of **evidence integrity and validity** during judicial procedures; [17]

3. Its deployment is **primarily facilitated by exploiting existing or created vulnerabilities** in digital systems (hardware or software), including by **social engineering, physical implantation or pre-installed mechanisms,**[18] **and deceptive ads;**[19]

4. After installation, its operation (i.e. giving commands) **is performed either automatically or remotely.** Once installed, the spyware operates without requiring further physical access to the device;

5. It can be **targeted** at individuals or groups, or deployed **indiscriminately**.

In addition, software that **serves to install spyware** as defined above equally falls into the definition (see section 2.1.4) – even if the former is not primarily intended for that purpose.

This characterisation avoids restrictive qualifiers like 'deliberately designed' or 'especially made', which would allow functionally identical tools to escape regulation simply because they are marketed differently.

A good precedent is the United States' (US) **Executive Order 14093,** which defines commercial spyware as any software that enables "remote access to a computer, without the consent of the user, administrator, or owner".[20] This broad approach ensures that emerging technologies and new surveillance methods remain covered by regulatory frameworks. Similarly, the European Union Agency for Cybersecurity (ENISA) defines spyware as "a type of malware that spies on users' activities' without their knowledge or consent, including keylogging, activity monitoring, and data collection".[21]

By contrast, narrower definitions, such as those in the **EU Dual-Use Regulation guidelines on cyber-surveillance tools,** fail to capture the full scope of spyware by focusing on the developer's intent and specific design features, rather than the tool's functionalities.[22]

16. Some spyware tools work by implanting executable code on the RAM in order to be imperceptible.
17. In judicial procedures, evidence must be reliable, authentic and verifiable. If the device was compromised, it becomes unclear whether evidence was altered, planted, deleted, wether the state of the device is authentic... Data cannot be trusted if the device from which it was obtained cannot be trusted.
18. We hold that the difference between physical implantation and pre-installed mechanisms is the knowledge and agreement of the manufacturer. An example of a pre-installed mechanism is the infamous Clipper Chip, a chipset developed and promoted by the United States National Security Agency (NSA) in the 1990s which would allow Federal, State, and local law enforcement agencies to the decrypt intercepted voice and data transmissions. Manufacturers were expected to implant the Clipper Chip in any new telephone or other device, in return for softer export controls. An example of physical implantation would be China's implantation of small malicious chips on motherboards of Super Micro Computer Inc. (Supermicro) starting from 2014 and affecting at least 30 U.S. companies downstream the supply chain from Supermicro including Apple and Amazon. See Bloomberg, "How China Used a Tiny Chip in a Hack That Infiltrated Amazon and Apple", October 4, 2018, *https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies*
19. *Haaretz*, "Revealed: Israeli Cyber Firms Developed an 'Insane' New Spyware Tool – No Defense Exists", September 14, 2023 *https://www.haaretz.com/israel-news/2023-09-14/ty-article-magazine/.highlight/revealed-israeli-cyber-firms-developed-an-insane-new-spyware-tool-no-defense-exists/0000018a-93cb-de77-a98f-ffdf2fb60000*
20. *Executive Order 14093*, "Prohibition on the Use of the United States Government of Commercial Spyware", March 27, 2023, *https://www.presidency.ucsb.edu/documents/executive-order-14093-prohibition-use-the-united-states-government-commercial-spyware-that*
21. Retrieved from *https://web.archive.org/web/20230419091714/https://www.enisa.europa.eu/topics/incident-response/glossary/malware*
22. The Commission described cyber-surveillance items as "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems". European Commission, "Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council", 2024, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402659*

2.1.3 The capabilities of spyware: what can this software do?

In addition to its core characteristics, spyware must be defined **by what it enables.** A software is considered spyware if, meeting the characteristics mentioned in 2.1.2., it enables **one or more** of the **following functionalities:**

→ **Accessing and monitoring the device (real-time data)**, enabling the operator of the spyware to observe activity, intercept communications, track location, etc., with potentially unlimited access;

→ **Gathering or processing user data (historical data)**, such as retrieving messages, call logs, browsing history, stored files, biometric information, etc.;

→ **Exfiltrating data** for the purpose of sharing that information with a third party;

→ **Controlling or manipulating the device,** such as activating microphones or cameras, altering system settings, disabling security features, etc.;

→ **Altering or fabricating information**, modifying, deleting, or fabricating messages, files, or logs to obscure or alter or-even plant-evidence.

This **either-or** approach is critical: a tool does not need to perform all these actions simultaneously to be classified as spyware.[23] **Any software meeting the core characteristics and that has one or more of these functionalities qualifies as 'spyware',** and therefore should fall **under the scope of a ban.**

Spyware's characteristics and capabilities make its use **inherently incompatible with the right to privacy.** This is because the use of these **tools violates the essence of this right, by compromising the integrity of a person's device without their consent and accessing a large volume of data in a way that is incompatible with the principles of necessity and proportionality** as required for any limitation of fundamental rights under the EU Charter.[24]

2.1.4 What falls under the categorisation of 'spyware'?

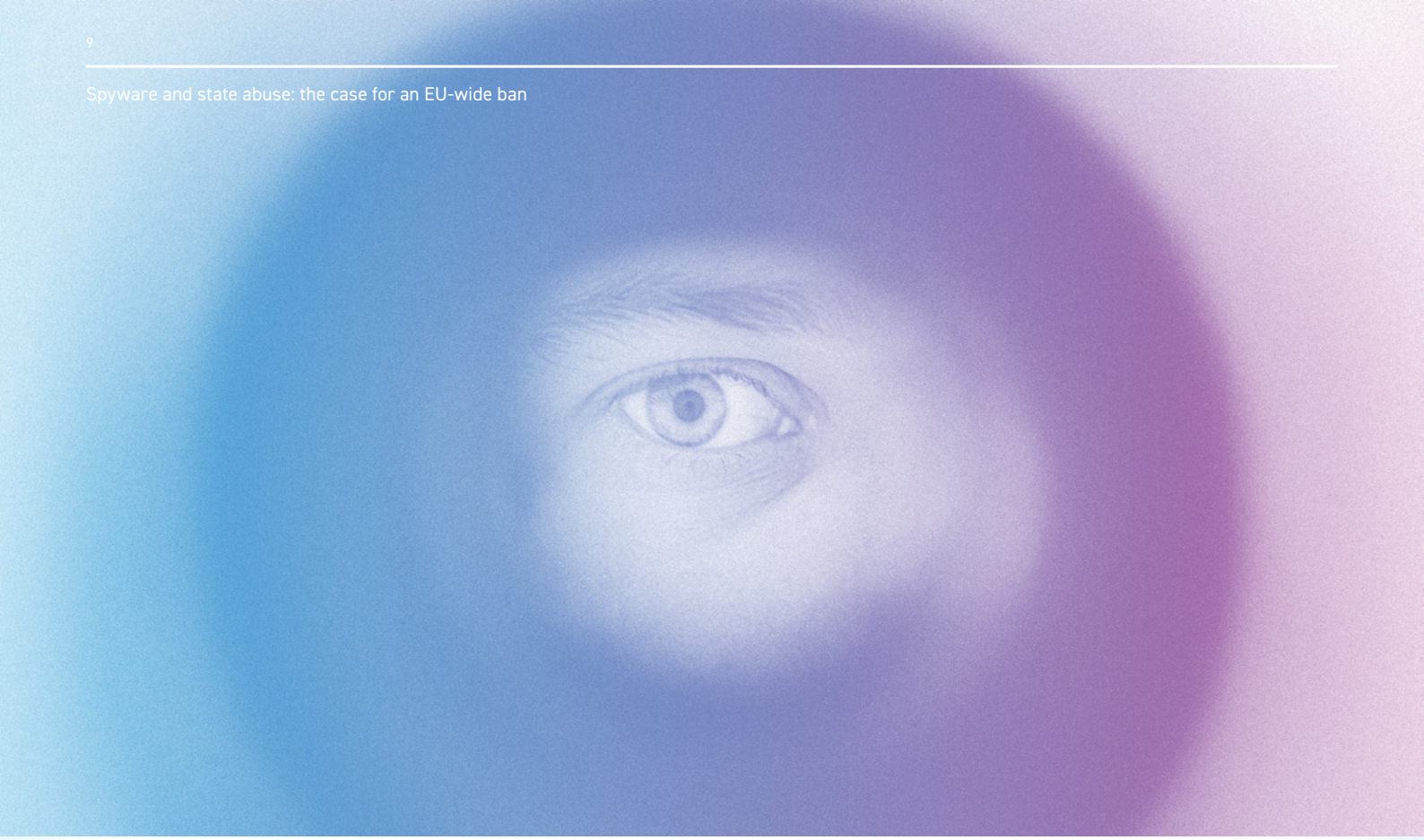
The following are non-exhaustive examples of tools that qualify as spyware under this definition:

→ **Commercial spyware:** spyware developed, produced and sold by private companies for government, corporate, or individual use. Notable examples include **Pegasus (NSO Group), Predator (Intellexa), Graphite (Paragon) or FinSpy/FinFisher (Lench IT Solutions PLC);**

→ **State-developed spyware:** some governments have begun developing their own spyware rather than relying on private vendors. Germany has been using its **"Remote Communication Interception Software (RCIS)**[25] for years now for law enforcement purposes, while France is currently developing its own.[26] In December 2024, Amnesty International revealed that the Serbian authorities were also using an in-house developed spyware called **"NoviSpy";**[27]

→ **Stalkerware:** spyware used by private individuals, often in intimate partner relationships, e.g. in cases of domestic violence, to surveil and control another individual. It is sometimes disguised as "parental control" software.[28]

23. A similar approach was taken by the Biden Administration in *EO 14093* , which defined spyware's capabilities as either: "(I) access, collect, exploit, extract, intercept, retrieve, or transmit content, including information stored on or transmitted through a computer connected to the Internet; (ii) record the computer's audio calls or video calls or use the computer to record audio or video; or (iii) track the location of the computer.
24. Charter of Fundamental Rights of the European Union, 2012/C 326/02, Article 52(1).
25. *Netzpolitik.org*, "Prüfbericht zum BKA-Staatstrojaner: Die Software ist- 2022, *https://netzpolitik.org/2022/die-software-ist-*
26. *Intelligence Online*, "French Intelligence Service Safeguards Funding for Developing In-House Spyware," February 3, 2025, *https://www.intelligenceonline.com/surveillance--interception/2025/02/03/french-intelligence-service-*
27. *Amnesty International*, "Serbia: A Digital Prison: Surveillance and the Suppression of Civil Society," December 2024, *https://www.amnesty.org/en/documents/eur70/8813/2024/en/*
28. *National Cybersecurity Alliance*, "Stalkerware," 2022, *https://www.staysafeonline.org/articles/stalkerware*



→ **Parental control or employee monitoring software:** while not all parental control tools are necessarily spyware, those that give an external party (parent, guardian or manager) remote, covert, and non-consentual access to, for example, a young person's or an employee's communications or device control settings, would fall under the definition of spyware. Software that would be strictly limited to blocking certain functionalities (like installing new apps) or blocking access to certain online contents would not qualify as spyware. As noted above, **parental control tools can often be used in situations of stalking** or digital coercive control;

→ **Keyloggers:**[29] programs that covertly record keystrokes to steal passwords, financial information, private communications, and employee activity.

→ **Infostealers:**[30] malware designed to extract sensitive user data, such as browser histories, stored credentials, and personal files. These are often used by **cybercriminals** but can also be leveraged by **state actors.**

2.1.5 What is not spyware?

The following are non-exhaustive examples of tools that do not qualify as spyware under this definition:

→ **Remote desktop software:** tools like KVM switches,[31] TeamViewer,[32] AnyDesk, or Microsoft Remote Desktop that are used for legitimate IT support and remote work. These require user consent before granting access, and can be revoked at any time;

→ **Exfiltration of low-sensitivity telemetry data:** software and operating system vendors collect telemetry data (such as error reports, usage statistics) for analytics and debugging in accordance with their Terms of Service and as part of their business practices. While privacy concerns exist when this is done poorly or excessively, these data are typically pseudonymised and the extraction does not grant wider device access;

29. *Malwarebytes*, "What Is a Keylogger?" 2024, *https://www.malwarebytes.com/keylogger*
30. *Proton*, "What Are Infostealers?" 2024, *https://proton.me/blog/infostealers*
31. *https://en.wikipedia.org/wiki/KVM_switch*
32. *www.teamviewer.com*

→ **Forensic tools:** such tools enable the copying or extraction of data stored on a given device without compromising its integrity – usually on unlocked devices. **The respect of the device integrity by digital forensic tools is crucial to meet criminal justice requirements of evidence integrity and validity:** digital evidence collected by investigative authorities needs to be reproducible and verifiable in court proceedings, including by the defence or independent technical experts. They **are considered spyware as soon as they are used to install spyware** as per the definition in section 2.1.2;

→ **Traditional methods of surveillance,** when undertaken in full in compliance with all applicable laws and safeguards. Theoretically, court-approved wiretapping or government access to data held by an internet service provider under established legal frameworks differ from spyware because they involve some level of oversight, transparency, and judicial control; are limited in scope and in the type and amount of data accessed,[33] which makes it potentially proportionate; and the access is not direct into the device, but through the cooperation of a third party – usually, telecom providers.[34]

2.1.6 Does it depend on who is using it?

The **focus of the definition of what 'spyware' is should be on the software's intrusive capabilities, rather than who is operating it. Our proposal for a ban is motivated by the disproportionate nature of spyware,** as this is what determines the impact on people's privacy and other human rights. Spyware remains spyware regardless of whether it is used by law enforcement agencies (LEA), intelligence services, private companies, cyber mercenaries or individuals, including abusive partners. However, there is of course **a higher burden on states to respect, protect and fulfil human rights,** meaning that we expect proactive action from state actors to protect our privacy from spyware, **and an obligation on companies** not to develop and sell rights-abusive tools.

2.1.7 The specific case of UFEDs

Although the infamous **Cellebrite Universal Forensics Extraction Device (UFED)**[35] markets itself as a traditional forensic tool, it actually **meets some of the core characteristics of spyware,** except for the possibility to have continuous data extraction after installation (unless Cellebrite is used to install spyware - see section 2.1.2 - which is illustrated by the 2024 spyware revelations in Serbia).[36] Cellebrite and similar software like MSAB's XRY[37] and **Magnet Forensics'** Graykey[38] compromise the integrity of locked devices by exploiting security vulnerabilities. For example, on locked devices, Cellebrite installs some executable code to the device,[39] either to brute-force[40] the password or to enable After First Unlock (AFU)[41] extraction. Therefore, Cellebrite does not limit itself to the simple extraction of data from devices as forensic tools do in the traditional sense. For that reason, and because of the risks entailed by such tools for fundamental rights, **EDRi believes the use of Cellebrite and Cellebrite-like software should also be prohibited.** While Cellebrite UFED and similar software is not directly in scope of the spyware ban advocated for by EDRi, the proposed **ban** on the vulnerabilities and exploit market in section 3.4 will also limit the uncontrolled use of UFEDs for data extraction insofar as this relies on exploiting device vulnerabilities.

33. On this issue, see the French Court's judgement declaring illegal the French law allowing its police and secret services to use spyware, in particular regarding to activating mics or cameras, due to its lack of compliance with necessity and proportionality requirements. Conseil Constitutionnel, "Décision n° 2023-855 DC du 16 novembre 2023 - Communiqué de presse," November 16, 2023, *https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2023-855-dc-du-16-novembre-2023-communique-de-presse*
34. *European Digital Rights (EDRi),* "Do You Trust the Police? CJEU Advocate General Accepts Access to Phones for Any Type of Crime," May 10, 2023, *https://edri.org/our-work/eu-court-of-justice-advocate-general-accepts-access-to-phones-for-any-crime/*
35. *Access Now,* "What spy firm Cellebrite can't hide from investors", 2021, *https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/*
36. *Amnesty International*, "Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists," December 16, 2024, *https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/*
37. *https://www.msab.com/product/xry-extract/*
38. *https://www.magnetforensics.com/products/magnet-graykey/*
39. The installation of the 'falcon' binary for data extraction is documented by Amnesty International in the report "Serbia: A Digital Prison: Surveillance and the Suppression of Civil Society," December 2024. *https://www.amnesty.org/en/documents/eur70/8813/2024/en/*
40. See Glossary
41. Smartphones have two different states that can affect the ability of unlocking them and extracting data from them."Before First Unlock" (BFU) – before the user has entered their passcode for the first time after powered on their device – stored data is fully encrypted. "After First Unlock" (AFU) – once the user successfully logs onto the phone after the device was powered off - certain data is unencrypted and may be easier to extract by some device forensic tools — even if the phone is locked. See *https://blogs.dsu.edu/digforce/2023/08/23/bfu-and-afu-lock-states/* for further discussion of BFU vs. AFU.

2.1.8 Comparison with traditional surveillance methods like bugging

Just like physical searches of a person's home, digital intrusions into personal devices should be subject to the strongest possible legal safeguards - because **accessing someone's phone today is often more intrusive than entering their house.**

But spyware used currently by European authorities is **fundamentally different from traditional surveillance techniques,** both in scope and intrusiveness. While older methods are usually **limited in time, space and data category,** spyware acts as an **all-in-one tool** that enables persistent, total access to a person's (digital) life. Compared to traditional methods:

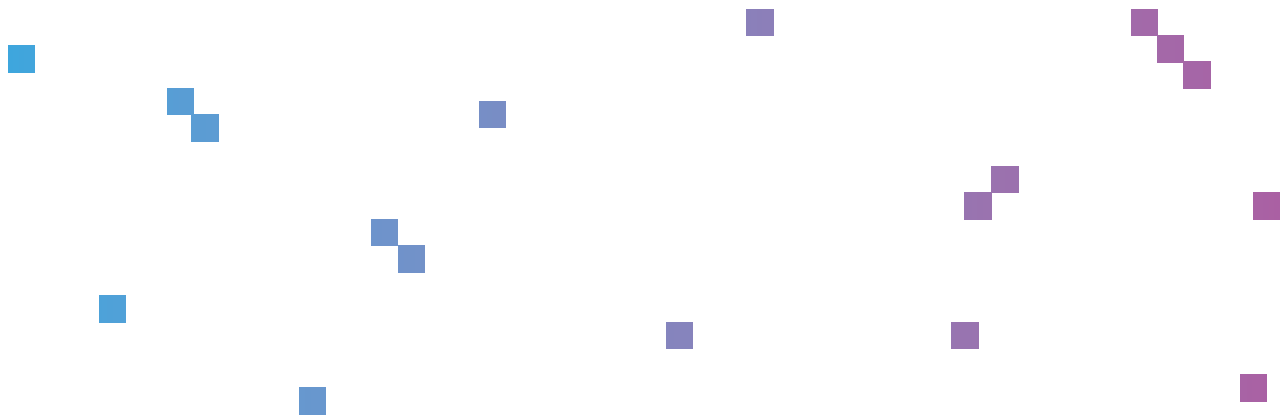
→ **Microphones and cameras** used in physical bugging are placed in fixed locations. Their placement is typically chosen to minimise the risk of collecting data from third parties (e.g. only recording the bedroom of a criminal suspect). By contrast, spyware can covertly turn on a device's microphone or camera regardless of the person's location, capturing continuous data from any environment, without it being targeted or limited, including from unsuspecting bystanders who are have no direct or indirect connection to the criminal investigation.

→ **GPS tracking** enables location surveillance but typically provides only one category of information – location – and may be device or object focused rather than person-focused. Spyware, however, tracks location alongside all other device activities, linking surveillance directly to a specific individual and numerous forms of information.

→ **House searches, even though they also give access to a huge amount of historic data,** are limited in time and scope. Authorities enter a particular space and collect what is physically present at that moment. This contrasts sharply with spyware, which can enable **continuous surveillance** and gathering of all historical and real-time data, over extended periods.

Spyware is therefore not just a digital equivalent of these methods – it can **combine and vastly exceed them.**

Furthermore, **the harm caused by spyware cannot be contained,** and often affects not only the target but also people who interact with them, both physically and digitally. This collateral intrusion is particularly problematic in criminal law, which is based on individual suspicion and accountability. This aspect of spyware has already been ruled unlawful by some courts.[42] Crucially, it also **compromises the device,** not allowing the evidence obtained from its use to pass any evidence integrity assessments in court. Its characteristics and capabilities make it **inherently incompatible with the principles of necessity, proportionality and legal safeguards.**



42. *Conseil Constitutionnel*, ibidem

2.2 Use of spyware by non-state actors: three case studies

State authorities are not the sole users of spyware. Spyware has become widely accessible and is increasingly used in private contexts, where its impacts on fundamental rights are still far-reaching.

A. Stalkerware and gender-based violence

A particularly insidious form of spyware is 'stalkerware', often misleadingly marketed as 'parental control' or 'employee monitoring' software. Tools like **PC Tattletale,**[43] **mSpy,**[44] and **TheTruthSpy**[45] allow private individuals and employers to covertly track (ex-)partners, employees and dissidents. The scale of abusive behaviour enabled by stalkerware has been exposed through data breaches affecting these widely-used spyware apps. In 2024, **TechCrunch**[46] reported that **mSpy** leaked millions of customer records, confirming its widespread use in **intimate partner surveillance.** Similarly, **LetMeSpy,** which specifically marketed itself for tracking individuals, was **hacked in 2023,** revealing tens of thousands of victims.[47] **Spyhide,**[48] **Spytech**[49] and **PC Tattletale**[50] also exposed data of more than 100,000 compromised devices.

The enabling factors behind the multiplication of stalkerware are a crucial lack of regulation, aggressive marketing practices that normalise digital surveillance and stalking,[51] and low prices. 'Low-cost' spyware tools can be purchased for as little as a few euros,[52] making them accessible to a wide range of abusers. At the same time, the risks they entail, ranging from coercive control to frequent data leaks, represent a serious threat to the safety, privacy and other human rights of affected people – especially placing women, LGBTQI+ people and other persons with marginalised identities at even greater risk.

Stalkerware is sometimes referred to as 'spouseware'[53] because it further enables gender-based violence (GBV), enabling abusers to monitor, control, and intimidate their partners. Investigations by IrpiMedia[54] and The Citizen Lab[55] show that these tools are often installed covertly by intimate partners or ex-partners, reinforcing patterns of abuse. This form of digital abuse is disproportionately committed by men against women,[56] many of whom are unaware that their devices have been compromised.

The EU's failure (and that of national governments) to ban commercial spyware has allowed companies to profit from GBV with near-total impunity. Survivors of digital abuse face enormous obstacles: detecting spyware, proving the violation, removing it safely, and navigating law enforcement systems that often fail to take action. A study conducted in seven Global Majority countries shows that 60% of reported cases of online violence against women are not investigated by authorities.[57] As reported by Amnesty International and the United Nations Development Program, this form of abuse creates long-term psychological, social, and security impacts.[58]

43. *TechCrunch*, "Spyware maker pcTattletale says it's 'out of business' and shuts down after data breach", 2024, *https://techcrunch.com/2024/05/28/pctattletale-spyware-shutters-data-breach/*
44. *https://www.mspy.com/*
45. *Business and Human Rights Resources Centre*, "TheTruthSpy spyware found on 50,000 Android devices", February 2024 *https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/thetruthspy-spyware-found-on-50000-android-devices/*
46. *TechCrunch*, "Data Breach Exposes Millions of mSpy Spyware Customers," 2024, *https://techcrunch.com/2024/07/11/mspy-spyware-millions-customers-data-breach/*
47. *TechCrunch*, "LetMeSpy Hacked: Spyware App Breach Exposes Thousands," 2023, *https://techcrunch.com/2023/06/27/letmespy-hacked-spyware-thousands/*
48. *TechCrunch*, "Spyhide Stalkerware is Spying on Tens of Thousands of Phones," 2023, *https://techcrunch.com/2023/07/24/spyhide-stalkerware-android/*
49. *TechCrunch*, "Spytech Data Breach Exposes Thousands of Compromised Devices," 2024, *https://techcrunch.com/2024/07/25/spytech-data-breach-windows-mac-android-chromebook-spyware/*
50. *IrpiMedia*, "PC Tattletale: Il Software di Spionaggio per Lavoratori," 2024, *https://irpimedia.irpi.eu/spiarelowcost-pc-tattletale-software-spyware-lavoratori/*
51. *Gesellschaft für Freiheitsrechte (GFF)*, "Cyberstalking-Apps: GFF reicht Beschwerde gegen Google bei der Bundesnetzagentur und der EU-Kommission ein," November 4, 2024, *https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-cyberstalking-google*
52. *IrpiMedia*, "La Zona Grigia del Mercato degli Stalkerware," 2024, *https://irpimedia.irpi.eu/spiarelowcost-app-parental-control-sorveglianza-elettronica/*
53. *BBC News*, "Stalkerware: The Software That Spies on Your Partner," October 24, 2019, *https://www.bbc.com/news/technology-50166147*
54. *IrpiMedia*, "Uomini che Spiano le Donne," 2024, *https://irpimedia.irpi.eu/spiarelowcost-stalkerware-donne/*
55. *Citizen Lab*, "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," 2019, *https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/*
56. *Kaspersky*, "Global Kaspersky Report Reveals Digital Violence Has Increased," 2024, *https://www.kaspersky.com/about/press-releases/global-kaspersky-report-reveals-digital-violence-has-increased*
57. *GenderIT.org*, "Tracking Online Gender-Based Violence," 2024, *https://genderit.org/onlinevaw/state/*
58. *Amnesty International*, "An Urgent Call to Address Online Gender-Based Violence," 2024, *https://www.amnesty.org/en/documents/asa39/7955/2024/en/; UNDP, "Tackling Gender-Based Violence in the Digital Age," 2024, https://www.undp.org/sites/g/files/zskgke326/files/2024-12/final-analysis-tf-gbv.pdf*

B. "Sextortion" and blackmail

The commercial spyware industry has also facilitated the rise of 'sextortion' networks, where survivors are blackmailed using stolen or coerced personal data - often sexual content, including intimate images, videos, or private conversations.

Furthermore, in 2020, the **Lookout Threat Intelligence** team discovered a spyware suite called **Goontact,** which lured individuals through illicit escort websites and prompted them to install malicious apps disguised as secure messaging tools.[59] Once installed, Goontact exfiltrated personal data - SMS messages, photos, contacts, location, images - and used it for extortion purposes. Victims were primarily targeted in China, Taiwan, South-Korea and Japan.

C. Spyware as a mercenary tool in geopolitical conflicts

Spyware has become a **weapon** in national or international conflicts, used by mercenary hackers – often, but not always, paid by governments - to extort or spy on a particular group of people, and as part of **hybrid campaigns of destabilisation.** For example, **APT15**, a Chinese hacking group allegedly tied to Chinese authorities,[60] deployed **BadBazaar**,[61] a spyware tool targeting **Tibetan and Uyghur communities.**

All these cases illustrate how **spyware use extends beyond so-called 'legitimate' state activities** – usually, via law enforcement and intelligence services, it is a tool of coercion and control used across public and private domains, and can additionally be used as a tool of **personal, corporate, and state-backed coercion.**

2.3 State use of commercial spyware

Many of the scandals regarding state use of spyware have involved the use of programs like **Pegasus, Graphite or Predator,** developed and sold by private vendors, with **particularly worrying capabilities:**[62]

→ **Unlimited data access:** These commercial spyware programs access and extract all historical and real-time data without constraint;

→ **Its use is not verifiable:** It leaves no clear log on the time or frequency of the infections, nor on the data obtained and its destination;

→ **Self-deletion:** Many spyware tools are designed to **self-delete** traces of use after operation, making forensic analysis and accountability difficult;

→ **Persistent control:** Spyware creates an **"invisible presence"** that is impossible for the average user to detect or remove, so it can persist for a long time on the person's device;

→ **Military design:** These tools were historically developed for military purposes, and are now used in civilian contexts. The problem is not only their technical capabilities, but also the fact that **they were never designed to operate within rights-respecting legal frameworks.** Its development and use in the occupied Palestinian territories[63] , in a context of military occupation, is a clear example of this.

59. Users were prompted to install a malicious app under various pretexts, like resolving audio or video issues. Lookout Threat Intelligence, "Lookout Discovers New Spyware 'Goontact' Used by Sextortionists for Blackmail," December 2020, *https://www.lookout.com/threat-intelligence/article/lookout-discovers-new-spyware-goontact-used-by-sextortionists-for-blackmail*
60. *ZDNet*, "Connection Discovered Between Chinese Hacker Group APT15 and Defense Contractor," 2020, *https://www.zdnet.com/article/connection-discovered-between-chinese-hacker-group-apt15-and-defense-contractor/*
61. *Lookout Threat Intelligence*, "BadBazaar: Surveillanceware Used by APT15 to Target Tibetan and Uyghur Communities," January 2024, *https://www.lookout.com/threat-intelligence/article/badbazaar-surveillanceware-apt15*
62. This is a non-exhaustive list that wants to highlight some particular threats to human rights of these spyware tools. As we have already mentioned, the omnipotent access, or any other of this listed capabilities is not a must characteristic of spyware. Spyware can have a limited access to the device, but can still fall under the 2.1 definition, and therefore under our call for a ban.
63. *The New Arab*, "How AI, Big Tech, and Spyware Power Israel's Occupation," 2023, *https://www.newarab.com/analysis/how-ai-big-tech-and-spyware-power-israels-occupation*

The chimera of 'good spyware'

The idea that there could be a 'good, rights-respecting spyware' is inherently flawed, as the very nature of the current state of play of spyware – **its unrestricted and secret access to devices, its use of vulnerabilities, its compromising of device integrity, and its military origins** - contradicts principles of transparency, accountability, **and fails to meet the standards of any fundamental rights impact assessment.** According to case law of the European Court of Human Rights (ECtHR),[64] any targeted surveillance, due to its impact on human rights, must be subject to clear legal frameworks, independent oversight, and strict **strict tests of necessity and proportionality.** However, spyware, **by design,** cannot meet these requirements.

Some relevant human rights experts have theorised on **which capabilities spyware should have, and how it should be deployed,** in order to be human rights compliant and have ex ante safeguards, such as:[65]

→ Allow deployers to **target only specific data ('surgical data extraction'),** rather than automatically monitor and record all data and metadata;

→ **Avoid automatically accessing data relating to contacts of targeted individuals,** unless justified;

→ Engineer mechanisms to prevent harmful use, such as flagging systems and **'kill switches'** in cases of apparent misuse;

→ **Logging all operator actions in an auditable, permanent record**

The reality is that **such technology does not exist today, and that it remains technically and practically infeasible.** Furthermore, it would rely on trusting actors that are intrisically trying to operate in the shadws. **There are no economic or political incentives** neither for vendors nor for states to develop such technical limitations. Finally, **reliance on technical solutions alone is inherently inadequate to address complex political issues,** such as the wide-ranging violations of human rights by state use of spyware.

The notion of 'human rights-compliant spyware' is therefore not a realistic route.

64. " in line with the case-law of the European Court of Human Rights on targeted surveillance, with respect to legality, legitimacy, necessity and proportionality of any surveillance measure". *Council of Europe*, "Pegasus and Similar Spyware and Secret State Surveillance," 2024, https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68rorism, "Position Paper on Global Regulation of Counter-Terrorism Spyware Technology Trade," December 2022, *https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf*

65. This comprehensive list of capabilities was drafted by the UN Special Rapporteur on Counter Terrorism: *UN Special Rapporteur on Counter-Terrorism*, "Position Paper on Global Regulation of Counter-Terrorism Spyware Technology Trade," December 2022, *https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf*

2.4 Policy recommendations to the European Commission

While national security remains the sole responsibility of the Member States under Article 4(2) of the Treaty on European Union, **this does not preclude EU action to legislate on spyware.** First of all, as the European Commission recently mentioned, national security cannot be a general justification, as it needs to meet a specific high threshold[66]. Furthermore, the development, production, marketing, sale, export, and use of spyware directly affect the functioning of the internal market, the **protection of fundamental rights enshrined in the Charter,** data protection, cybersecurity, and the EU's external relations, all of them areas squarely within EU competence. A full ban on spyware would not interfere with Member States' national security prerogatives, but rather establish **uniform rules to prevent the proliferation and abuse through these tools across the Union** and abroad.

EDRi calls for a full ban on the development, production, marketing, sale, export, and use of spyware as the only acceptable, human rights-compliant solution.

1 **Full ban on spyware. The European Commission should, propose a full ban on the development, production, marketing, sale, export, and use of spyware,** as a matter of urgency.

2 **Legally robust definition of spyware. This ban must be based on a clear and enforceable definition of spyware, focusing on its core characteristics and functionalities rather than its marketing or intended use.** Only such a comprehensive approach can prevent abuse, ensure legal certainty, and uphold the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union.

3 **Comprehensive scope covering all actors. The prohibition must cover all public and private actors operating within the EU or subject to its jurisdiction.** It should not be limited to tools used by states in law enforcement or national security contexts, but must also encompass commercial spyware marketed for other uses, including corporate or private surveillance.

66. According to the CJEU, the term 'national security' refers to 'the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities. EU Commission, "Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)", *https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act*

3. ABUSE FOR SALE: PUTTING AN END TO THE PROLIFERATION OF COMMERCIAL SPYWARE

The commercial spyware market enables states to access highly intrusive surveillance capabilities without the need to develop them in-house. A growing number of private companies are building and selling such tools, sometimes to a handful of state actors, sometimes to dozens. These actors operate in a legally and ethically ambiguous space: formally private, often composed of ex-military actors, and deeply connected to security establishments.

Because they are privately run, **commercial spyware vendors** pursue before anything. In practice, this means **operating in secrecy, exploiting human rights for profit,** and **enabling mass rights violations** across jurisdictions.

The **spyware industry** is not only inherently harmful in its impact, but also **dangerous by design. Its business model depends on the abuse of software vulnerabilities, a practice that weakens cybersecurity for everyone.** Human rights violations occur not only at the point of deployment, but throughout the entire lifecycle—from development to marketing, sale, and post-sale 'support'.

3.1 The proliferation problem: how the commercial market has made spyware cheaper and more accessible

Hacking into devices has never been an easy task for state authorities. An operative intrusion plan usually includes the search for vulnerabilities in the digital infrastructure (hardware, software and networks), development of exploits and spyware implants, and identification of adequate attack vectors. **It requires considerable economic resources,** time and expertise before the targeted system can be effectively compromised. This explains the discrepancy between countries' capabilities in this area and why some possess more elaborate techniques than others.

The emergence and expansion of the commercial spyware market has significantly changed this capability-gap.[67] Purchasing off-the-shelf spyware is now relatively inexpensive – especially for state actors. According to a report in The New York Times, Pegasus costs a bit more than 1 million dollars for ten targets.[68]

The UK's intelligence, security and cyber agency reported that **more than 80 countries have purchased spyware** and "warned that the proliferation of these commercial hacking tools and services **was further lowering the barriers to entry for state and non-state actors in cyberspace."**[69] This is consistent with data from the Carnegie[70] global inventory of commercial spyware and digital forensics, which indicated that **74 countries have acquired commercial spyware.** Countries which previously lacked the resources and sophistication to conduct hacking domestically (including those with a dictatorial or repressive regime) can now turn to the commercial surveillance industry to carry ouy unlawful surveillance using spyware.

The other side of the coin is that **commercial spyware has become a lucrative business,** generating around 12 billion dollars a year.[71] For example, the Israeli firm Paragon was acquired in 2024 by an investment firm in a deal worth up to 900 million dollars.[70] In parallel, the **vulnerabilities market**[73] **continues to flourish,** with growing demand. *TechCrunch* reported that a startup called Crowdfense gradually raised prices for its zero-day exploits[74] over the past years: between 5 and 7 million dollars for exploits targeting iPhones; up to 5 million for Android phones; up to 3 and 3.5 million for Chrome and Safari respectively; and 3 to 5 million dollars for WhatsApp and iMessage, making the development and sale of spyware a lucrative opportunity.[75]

Private companies are behind the most sophisticated hacking and surveillance tools currently on the market and thus pose aserious threat to our collective security and privacy online. However, the **uncontrolled proliferation of such weapons**[76] and the mainstreaming of their use **are the responsibility of states,** which have repeatedly failed to take appropriate measures to eliminate the profit incentives of this intrusion-as-a-service market. A clear example of this lack of control is explained by Google's Threat Analysis Group, which has tracked 40 commercial surveillance vendors: "While these vendors claim to vet their customers and usage carefully with the promise that their work is only used to target criminals and terrorists, what we have observed time and time again is [...] **that these tools are used by governments for purposes at odds with democratic values".**[77]

Although the EU takes pride in its advanced data protection and privacy rules, reports point to the worryingly **favourable business environment that the EU offers to commercial spyware vendors.**[78] The European Parliament noted in 2023 that "many spyware developers and vendors are or have been registered in one or more Member States", citing **Thalestris Limited** (the parent company of Intellexa) in Ireland, Greece, Switzerland and Cyprus, **DSIRF** in Austria, **QuaDream** in Cyprus, Amesys and **Nexa Technologies** in France, and **FinFisher** in Germany.[79] We can now add to the list companies such as **Paragon**, in Germany,[80] or **Paradigm Shift, Palm Beach Networks** and **Epsilon,** companies based in Barcelona.[81]

This is also why Italy has attracted significant criticism in recent years, notably for being home to six known spyware producers in Europe.[82] In this context, an investigation has revealed the role played by public procurements in the development of a nefarious spyware market and in the accessibility and multiplicity of tools.[83] Indeed, **prosecuting authorities in Italy authorise far more surveillance operations each year than their to European counterparts.**[84] In other words, it seems that the supply may shapes the demand.

67. It is reported that the Israeli NSO Group has 60 government agency clients in 40 countries. The Washington Post, "On the list: Ten prime ministers, three presidents and a king," 20 July 2021, *https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/*
68. Citing a 2016 price list, the New York Times reported the NSO Group charged its customers $650,000 to infiltrate 10 devices, plus plus an installation fee of $500,000. New York Times, "How Spy Tech Firms Let Governments See Everything on a Smartphone," 2 September 2016, *https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html*
69. *The Record*, "More than 80 countries have purchased spyware, British cyber agency warns," 19 April 2023, *https://therecord.media/spyware-purchased-by-eighty-countries-gchq-warns*
We are aware that, as part of the Five Eyes and one of the only states in the world with enough capacities and resources to develop in-house hacking techniques, the UK has vested interests in maintaining this comparative advantage and is therefore worried that other countries are now able to acquire similar surveillance capabilities.
70. *Mendeley Data Feldstein*, Steven; Kot, Brian, "Global Inventory of Commercial Spyware & Digital Forensics", 2023, *https://data.mendeley.com/datasets/csvhpkt8tm/10*
71. *Carnegie Endowment for International Peace*, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," March 14, 2023, *https://carnegieendowment.org/research/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses*
72. *Calcalistech*, "Spyware startup Paragon acquired for up to $900M by investment firm AE", 2024, *https://www.calcalistech.com/ctechnews/article/s1ucev64kg*
73. See Glossary
74. See Glossary and EDRi, "State access to encrypted data," October 2022, *https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf*
75. *TechCrunch*, "Price of zero-day exploits rises as companies harden products against hackers," 6 April 2024, *https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/* The articles notes that "Crowdfense currently offers the highest publicly known prices to date", except for a Russian company.
76. We deliberately use this term given the role played by spyware in serious repressive and offensive operations, such as the murders of Jamal Khashoggi and Cecilio Pineda Birto – see, The Guardian, "Revealed: murdered journalist's number selected by Mexican NSO client," 18 July 2021, *https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto*
77. *The Record*, "Commercial spyware on the agenda as UN Security Council members meet," 2024, *https://therecord.media/commercial-spyware-meeting-un-security-council-members* Shane Huntley also said: "Well-known companies peddling spyware such as the NSO Group get all the headlines, Huntley said, but dozens of smaller vendors are contributing to the problem"
78. *Politico*, "How Europe Became the Wild West of Spyware," 25 October 2023, *https://www.politico.eu/article/how-europe-became-wild-west-spyware/*
79. *European Parliament*, "Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP))," *https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html*
80. *Euractiv*, "EXCLUSIVE: Spyware firm behind new surveillance of journalists, civil society operates from the EU", 2025, *https://www.euractiv.com/section/tech/news/exclusive-spyware-firm-behind-new-surveillance-of-journalists-civil-society-operates-from-the-eu/*
81. *TechCrunch*, "How Barcelona became an unlikely hub for spyware startups," 13 January 2025, *https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/*
82. IrpiMedia, "Italian spyware on the international market," 21 March 2023, *https://irpimedia.irpi.eu/en-italian-spyware-on-the-international-market*
83. *IrpiMedia, Ibid*
84. *IrpiMedia, Ibid*

In 2024, *Haaretz* and *TechCrunch* revealed the relocation of Israeli hackers and the establishment of new spyware companies in Catalonia.[85] One of the reasons for this relocation to Europe is the tightening of export rules in Israel following highly-publicised scandals involving the NSO Group. As stated by TechCrunch, **"it is now more difficult for companies to export spyware from Israel to the rest of the world, including the European Union, than from within the bloc itself."**[86] It seems that the EU provides, at the time of writing, a **more permissive business environment for spyware vendors,** due to its low trade barriers within the bloc and its relatively weak controls on dual-use exports. Instead of preventing it, **EU rules are fostering the proliferation of commercial spyware,** which is subsequently used to violate human rights around the world.

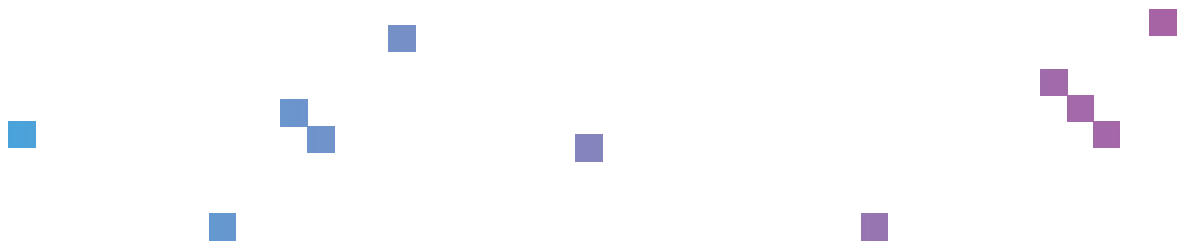
Spyware developers rely on zero-day vulnerabilities to infiltrate targets without detection. This vulnerabilities – that put as all at risk, and can be used against anyone, including state interests – are crucial for the spyware industry. **Ironically, public funding largely fuels the zero-day vulnerabilities market,** both by increasing demand in the commercial spyware market, and by directly investing in finding vulnerabilities. On the latter, some EU Member State governments allocate a part of their budgets for paying security researchers to find zero-day vulnerabilities for exploitation and in-house spyware deployment. For example, the company Zerodium acts as intermediary between security researchers and government institutions mainly in Europe and North America, keeping both sides of the transaction anonymous to each other.[87] Zerodium currently offers payments up to **2.5 million dollars for vulnerability information, substantially higher than the bug bounty programmes**[88] **of the software industry. Public funding** that supports these large payments from Zerodium (and other intermediaries in the lucrative trade of vulnerability information for exploitation) should, wherever possible, **be redirected to fixing security vulnerabilities** before they are exploited by malicious actors.

The current legal and political situation at best ignores - and at worst, facilitates and supports - the design, development, and deployment of commercial spyware technologies. It must be urgently reformed through a ban on the commercial spyware market.

3.2 Unacceptable risks posed by the commercial spyware market

"By keeping vulnerabilities [in computer systems] open, or even creating them, those resorting to hacking **may contribute to security and privacy threats for millions of users** and the broader digital information ecosystem."- Report of the Office of the United Nations High Commissioner for Human Rights, 2022. [89]

The commercial spyware industry, by its very nature, **represents a systemic threat** not only to human rights, but **also to cybersecurity, democratic stability, and global safety.** This concerns not merely of how spyware is used, but how it is designed and how the industry functions. From development through to marketing and deployment, the spyware business model is predicated on secrecy, impunity, and exploitation of vulnerabilities.



85. *Haaretz*, "'Expulsion to Spain': Israeli Hackers Flock to Barcelona in Big Spyware Shift," 26 December 2024, *https://www.haaretz.com/israel-news/security-aviation/2024-12-26/ty-article/.premium/israeli-hackers-flock-to-barcelona-as-spyware-industry-shifts/00000193-fec4-df5b-a9b3-fec5d9dc0000*
86. *TechCrunch, Ibid*
87. *Zerodium*, "Zero-day Exploit Acquisition Platform," accessed 2025, *https://zerodium.com*
88. See Glossary
89. *Office of the United Nations High Commissioner for Human Rights*, "The Right to Privacy in the Digital Age," 4 August 2022, *https://docs.un.org/en/A/HRC/51/17*

A. The vulnerabilities market, a threat to cyber- and national security

Spyware primarily functions by exploiting vulnerabilities. These include deliberately created flaws, such as government backdoors, and those acquired on a thriving market that exploits security flaws, like zero-days and other unpatched vulnerabilities. **Instead of resolving them, spyware vendors - and often states themselves - choose to weaponize them. This leaves users, including public officials, chronically vulnerable.**

Recent reports confirm **how dangerous the mandated backdoors approach is:** the Chinese hacking group Salt Typhoon reportedly accessed backdoors created for lawful interception, and maintained access to critical US telecom infrastructure "for months or longer," with unknown consequences.[90] **This dangerous outcome is not an exception, but is enabled by design.**

What's more, **the effect of commercial spyware vendors on the vulnerabilities market is clear: they do not just take advantage of this market, they actively fuel it.** According to Google's Threat Analysis Group (TAG), **twenty out of twenty-five zero-day vulnerabilities identified in 2023 were exploited by commercial spyware vendors.**[91] This staggering figure makes clear that commercial spyware is the main driver of exploit demand.

The result is a systemic security failure, **where governments and private actors incentivise insecurity, rather than strengthening the digital ecosystem.** The multiplication of commercial spyware vendors, **results in an increase in unknown vulnerabilities in digital systems,** posing a direct, substantial threat to everyone's online safety and privacy. **This includes state officials and governmental administrations who rely on the same digital systems to operate and to protect confidential and secret information.**

The need for bug bounty programs

This concerning dynamic also **sidelines genuinely ethical cybersecurity research.** Vulnerability brokers such as **Zerodium** and **Crowdfense** offer millions for zero-day exploits,[92] vastly outbidding **public bug bounty programmes**[93]**.** This deprives developers of the opportunity to patch flaws, as researchers are financially more rewarded for secrecy than for disclosure. **As a result, the security of states** and of their citizens and residents is at risk, and **largely depends on the ability and willingness of vendors and manufacturers to find vulnerabilities** and provide swift security patches.

This billions-dollars spyware-industrial complex[94] is eroding the very foundations of cybersecurity by keeping vulnerabilities open, legitimizing offensive cyberweapons, and outsourcing control to private actors with no incentive to prioritise rights or resilience.

The EU cannot contribute to weakening cyberspace

Of course, it's true that if the EU bans this market, companies and developers will move elsewhere. The spyware industry's reliance on jurisdictional arbitrage allows vendors to exploit regulatory gaps, perpetuating the vulnerabilities market[95]. By relocating to countries with lax oversight, these companies can continue to trade in zero-day exploits with minimal accountability. **But the EU cannot use that as an excuse to allow this market, which undermines its internal security and the global cybersecurity scenario.** And the EU does have some power: companies locate themselves partly on where their developers are willing to live. Barring companies from settling in Europe, would make it more difficult for them to attract developers.

By contributing actively or passively to the exploit market – through the absence of robust regulatory actions and the tolerance towards investors – **the EU is shooting itself in the foot and weakening its own security.**

90. *Techdirt*, "A 25-Year-Old Is Writing Backdoors Into The Treasury's $6 Trillion Payment System. What Could Possibly Go Wrong?", 5 February 2025, *https://www.techdirt.com/2025/02/05/a-25-year-old-is-writing-backdoors-into-the-treasurys-6-trillion-payment-system-what-could-possibly-go-wrong*
91. *The Record*, "Commercial spyware on the agenda as UN Security Council members meet," 2024, *https://therecord.media/commercial-spyware-meeting-un-security-council-members*
92. *LTechCrunch*, "Price of zero-day exploits rises as companies harden products against hackers," 6 April 2024, *https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/*
93. *See Glossary*
94. See part 3.1 for data on the market's revenue
95. *Atlantic Council*, "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights," 2023, *https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them*

B. Transparency and liability issues

When it comes to human rights due diligence and despite their feigned commitments to corporate responsibility (such as to the UN Guiding Principles for Business and Human Rights), **commercial spyware vendors largely operate with virtually no oversight and a complete lack of transparency.**[96]

The spyware industry thrives in opacity. Vendors disguise their tools under vague labels like "lawful access" or "investigative technology"[97] and operate through layers of shell companies to facilitate investment and erode liability.[98] As a result, transparency is nearly impossible to establish, and most information we have has to be provided by investigative journalists. In addition to this, investors are fully backing this opaque spyware economy. Paragon's recent acquisition by a U.S. private equity firm for up to 900 million dollars shows the massive scale of this surveillance-as-a-service model.[99] **Profit is driving the expansion of this market, not security or justice.**

Further complicating the situation is the complexity of determining **who is accountable:** it is often unclear who is responsible for what across the transnational chain of production, making it **almost impossible to provide remedies to victims** and hold those responsible accountable.[100]

3.3 How is the current EU legislation allowing the proliferation of commercial spyware?

As we observe a trend of companies relocating to and opening in Europe, we must examine the current EU legislative landscape in order to understand the **legal conditions under which the commercial spyware market is flourishing within EU territory.**

A. The Dual-Use Regulation and its shortcomings

Since 1994, the EU has regulated the export of "dual-use items" - goods, software, and technologies usable for both civilian and military purposes.[101] The most recent update of this law was adopted in 2021. Cyber-surveillance tools formally fall under this framework,[102] including "intrusion software", "communication monitoring software" or "forensic tools".[103] In 2024, the Commission issued specific guidance on how the Regulation should apply to cyber-surveillance exports and, therefore, to spyware exports.[104]

However, despite the Guidelines, the Regulation **is fundamentally unfit to address commercial spyware proliferation for the following reasons:**

96. *UN Human Rights Council,* "Report on Business and Human Rights," A/HRC/41/25, May 2019, *https://undocs.org/A/HRC/41/25*
97. *Atlantic Council, Ibid*
98. *Politico,* "Europe's Pegasus scandal: EU probe targets NSO," 2022, *https://www.politico.eu/article/europe-pegasus-spyware-eu-probe-nso/*
99. *The Record,* "Paragon bought by U.S. private equity," 2024, *https://therecord.media/paragon-bought-private-equity-american*
100. *UN Special Rapporteur on Counter-Terrorism,* "Position Paper on Global Regulation of Counter-Terrorism Spyware Technology Trade," December 2022, *https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf*
101. *European Union*, "Regulation (EU) 2021/821," *https://eur-lex.europa.eu/eli/reg/2021/821/oj*
102. *Michel, Quentin et al.,* "A Decade of Evolution of Dual-Use Trade Control Concepts," European Studies Unit, University of Liège, 2020, *https://orbi.uliege.be/bitstream/2268/246711/1/full.pdf*
103. This terminology for cyber-surveillance items was updated in 2024, *European Commission,* "RECOMMENDATION (EU) 2024/214 of 10 January 2024 on guidelines setting out the methodology for data gathering and processing for the preparation of the annual report on the control of exports, brokering, technical assistance, transit and transfer of dual-use items ", *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32024H0214*
104. *European Commission,* "Guidelines for Cyber-Surveillance Exporters," 16 October 2024, *https://policy.trade.ec.europa.eu/news/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en*

1. **Limited scope: export control only.** The regulation applies exclusively to **exports** outside the EU. Also, the EU's regime **lacks extraterritorial reach,** which further limits the control of spyware proliferation via subsidiaries or resellers;

2. **Internal trade is free.** Only those items that are listed under "Annex IV - Very Sensitive Items" of the Dual-Use regulation are subject to licensing when exported from one EU Member State to another. Therefore, the internal market of commercial spyware – which is part of "Annex I – List of Dual-Use Items" - is at the moment a totally free market with no regulations or need for licences;

3. **Weak enforcement and oversight.** The Commission's 2024 guidelines fail to establish strong safeguards. Specifically:

   → The export controls apply **only to products that have caused or can cause "serious human rights or international humanitarian law (IHL) violations" in third countries.** This creates a major gap where systems have led to harm in the EU. In general, as highlighted by many CSOs, **the text fails to provide criteria for interpreting what constitutes a "serious" human rights violation,** and "the existing criteria in place for military technology or equipment lack robust interpretation, implementation, and enforcement across the EU".[105]

   → Even when such risks exist, there is **no automatic suspension mechanism for exports,** as exporters are merely required to conduct a **human rights self-assessment;**

4. Enforcement is also weak partly because **implementation and licensing decisions are left to Member States,** as well as the application of the "human rights catch-all clause[106]", so there are no common criteria regarding that.

The Wassenaar Arrangement[107]**,** which develops control lists that inform the EU's Double-Use regulation, is also highly flawed. It has been described as ineffective[108] - dominated by geopolitical considerations, with key players like China not participating and countries like Russia blocking any updates. **At the time of writing, the Arrangement is still a non-binding list that has been stalled for years.**

An easy first step to improve the current situation **would be to step up the enforcement of the Dual-Use Regulation and the Commission's 2024 guidelines, with a strict human rights-compliant interpretation.** Second, controls and monitoring could be tightened by **listing spyware under Annex IV,** which would make it subject to licensing systems also for intra-EU trades.

However, in light of its narrow scope, weak internal controls, and lack of enforceability, the **Dual-Use Regulation is not a suitable legal instrument to effectively regulate the commercial spyware market, and has failed** to prevent the supply of commercial spyware to authoritarian regimes around the world.[109]

B. Weapons legislation, a missed opportunity?

Spyware could be treated by states similarly to conventional weapons[110], and its commercial proliferation addressed through strong legal regimes.

The EU has, over time, developed a framework for the trade of both civilian and military weapons. Civilian firearms fall under the Firearms Directive (Directive (EU) 2021/555),[111] which sets certain controls on acquisition, possession, and intra-EU transfers. Military weapons are regulated by the Council Common Position 2008/944/CFSP,[112] which in theory requires EU Member States to assess all exports against criteria such as human rights, security, and regional stability. This framework includes a "Common Military List" that does not include 'spyware' per se, but includes categories (such as 'intrusion software') that could encompass spyware.[113]

105. *Access Now*, "Analysis of EU Surveillance Tech Export Rules," 2021, *https://www.accessnow.org/wp-content/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf*
106. *BAFA*, "Leaflet on Art. 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821)" *https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_leaflet_art-5_eu-dual-use-regulation.pdf?__blob=publicationFile&v=2*
107. *https://www.wassenaar.org/*
108. *Austin Lewis*, "The Effectiveness of the Wassenaar Arrangement as the Non-Proliferation Regime for Conventional Weapons", 2015, *https://stacks.stanford.edu/file/druid:mz349xm4602/The%20Effectiveness%20of%20the%20Wassenaar%20Arrangement%20as%20the%20Non-proliferation%20Regime%20for%20Conventional%20Weapons%20-%20Austin%20Lewis.pdf*
109. *Spiegel*, "The Predator Files: European Spyware Consortium Supplied Despots and Dictators," 2023, *https://www.spiegel.de/international/business/the-predator-files-european-spyware-consortium-supplied-despots-and-dictators-a-2fd8043f-c5c1-4b05-b5a6-e8f8b9949978*
110. As mentioned in footnote 72, spyware can be equated to a weapon due to its severe and often irreversible impact on victims: it has been used to suppress dissent, dismantle democratic opposition, and has contributed to grave human rights violations, including arbitrary detention and even killings.
111. *European Union*, "Directive (EU) 2021/555," *https://eur-lex.europa.eu/eli/dir/2021/555/oj/eng*
112. *European Union*, "Council Common Position 2008/944/CFSP" *https://eur-lex.europa.eu/eli/compos/2008/944/oj/eng*
113. *European Union*, "Common Milityary List of the European Union", adopted on February 2020 *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XG0313(07)*

Spyware's origin lies in military intelligence and occupation, notably in contexts like the occupied Palestinian territories,[114] and **it has been used in war zones**[115] and against human rights defenders and populations seeking liberation from occupation forces.[116] But integrating spyware into this existing military export framework would have similar shortcomings as the Dual-Use Regulation:

→ The internal EU trade of weapons remains unlicensed - only exports to non-EU countries are scrutinised by this legislation; the internal EU trade of military items is generally unlicensed,[117] unless national rules or security exceptions apply.

→ Responsibility lies with Member States to issue export licences, based on "prior knowledge of end use in the country of final destination". In practice, EU states often approve such licences even when there are credible risks of rights abuses.[118]

C. The Pall Mall Process

The Pall Mall Process,[119] initiated in February 2024 by the United Kingdom and France, aims to address "the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCICs)".[120] Their concerns focus on "how commercial spyware undermines national security, human rights, international peace, and the stability of cyberspace".

However, as of the first half of 2025, the Pall Mall Process has only produced two non-binding documents: a declaration and code of practice for states.[121] **While these documents may outline good intentions, their voluntary nature raises serious doubts about their effectiveness** in curbing abuses or change policies or practices in the twenty-five states involved (of which eighteen are EU Member States). Furthermore, **they also appear to legitimise certain types of spyware and use cases.**

In addition, the Pall Mall process also foresees a **voluntary code of practice for spyware vendors.** But the effective implementation of such codes by vendors **is highly uncertain.** As noted by one of the companies involved, "the challenge remains of how the Pall Mall Process [...] will actually reach those whose behaviours and conduct needs to change to make a real difference."[122]

The Western-centric leadership by the UK and France has also limited global buy-in, with around twenty signatories to the voluntary code at the time of writing this paper. The absence of the United States - due to its withdrawal under the second Trump administration - further weakens the process. As highlighted in its own consultation summary, a lack of representation in the Process risks disengagement: "If states or stakeholders in different regions do not feel represented, this might lead to withdrawal or disengagement". [123]

In its current form, **the Pall Mall Process risks falling drastically short of its goals**. To be truly effective, it must move beyond voluntary frameworks and evolve into a **binding, enforceable agreement that directly addresses the human rights consequences of commercial spyware practices.** Otherwise, it will remain a diplomatic exercise detached from the realities of the industry and the profound harms it is causing.

114. *Chatham House,* "Review: Why Israel tests its spyware on Palestinians", November 2023 *https://www.chathamhouse.org/publications/the-world-today/2023-06/review-why-israel-tests-its-spyware-palestinians.*
115. *Access Now,* "Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict", May 2023 *https://www.accessnow.org/press-release/spyware-warfare-pegasus-in-azerbaijan-armenia-conflict/*
116. *Amnesty International*, "Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict", 2021 *https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/*
117. Intra-EU transfers of military equipment are governed by Directive 2009/43/EC. No export licence is needed for intra-EU transfers of many military items if the supplier uses a general or global transfer licence.
118. *Chiara Bonaiutti,* "Arms Transfers and Human Rights: Assessing the Impact and Enforcement of the EU Common Position on Arms Exports in a Multilevel Analysis", 2024, *https://www.researchgate.net/publication/366958609_Article_Arms_Transfers_and_Human_Rights_Assessing_the_Impact_and_Enforcement_of_the_EU_Common_Position_on_Arms_Exports_in_a_Multilevel_Analysis*
119. *Ministry for Europe and Foreign Affairs (France),* "The Pall Mall Process," 2024, *https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of*
120. According to the Code of Practice for States, "The market for CCICs encompasses a wide variety of cyber intrusion companies offering products and services that are continually evolving and diversifying, including those for computer system penetration or interference in exchange for commercial benefit and/or released under a free and open-source licence, such as commercial intrusive surveillance software (sometimes referred to as commercial spyware), and the vulnerabilities and exploits marketplace". *UK Government,* "The Pall Mall Process: Code of Practice for States," *https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states*
121. *Ibid*
122. *The Record,* "Pall Mall Process to tackle commercial hacking proliferation raises more concerns than solutions", 2025 *https://therecord.media/pall-mall-process-commercial-hacking-concerns*
123. *Pall Mall Process,* Consultation on good practices: summary report. 2025 *https://assets.publishing.service.gov.uk/media/677e486ed721a08c00665555/Pall-Mall-Process-Consultation-Summary-Report.pdf*

D. Are the CRA and NIS2 useful tools for regulating the vulnerabilities market?

In response to the increasing threats to cybersecurity, the EU has introduced new instruments such as **the Cyber Resilience Act (CRA)** and the revised **Network and Information Security Directive (NIS2)**. While both aim to strengthen the digital ecosystem and address systemic vulnerabilities, they fall short in terms of regulating the commercial spyware market.

The CRA[124], adopted in 2024, introduced essential cybersecurity requirements for "products with digital elements." It obliges manufacturers to patch known vulnerabilities, conduct risk assessments, and ensure transparency about software integrity. The CRA is a significant and positive step forward for the EU's digital policy - but it has key limitations when it comes to spyware:

→ **Scope exclusion**: The CRA does not apply to national security or defence-related products. Spyware developed or used by public authorities is thus excluded. Commercial spyware vendors often position their tools as "law enforcement tools" or "investigative solutions," which places them outside the consumer product scope.

→ **Lack of enforcement on deliberate vulnerabilities:** The CRA primarily targets accidental flaws and negligence. It does not cover vendors who deliberately exploit or commercially trade in vulnerabilities for offensive purposes.

One possible avenue of action is to explore if the CRA could be leveraged to harden devices against exploits, as well as to ban products, such as stalkerware, which are readily available off the shelf to any consumer. This would still not, however, represent a comprehensive solution.

The NIS2 Directive, adopted in 2022, expands the cybersecurity obligations of entities operating in eighteen sectors across the EU market - including digital services, energy, health, and public administration. It introduces stricter requirements for incident reporting, risk management, and supply chain transparency. However, like the CRA, it has limited utility in addressing spyware:

→ **Focus on resilience, not abuse:** NIS2 aims to prevent disruptions to infrastructure, rather than to address the covert surveillance of individuals or human rights abuses.

→ **No specific rules for surveillance tech:** There is no mandate to regulate vendors developing tools that compromise security or exploit vulnerabilities.

→ **Exemptions for state use:** National security operations – which is how state use of spyware is often framed - fall outside the directive's scope.

While both the CRA and NIS2 are critical to enhancing the EU's digital ecosystem, they are n**ot suitable mechanisms to regulate the commercial spyware market.** They focus on risk prevention and resilience, whereas spyware is a **deliberate and systemic threat** that targets users' rights, safety, and digital infrastructure. It is also important to critically highlight that both texts include massive loopholes on the basis of **national security claims,** which prevents both pieces of legislation (and other EU legal acts) from effectively and comprehensively disrupting the spyware market.

E. Sanctions on vendors and investors

Sanctions against commercial spyware vendors and investors **may not constitute a long-term solution.** However, they can produce some positive short-term effects, such as those implemented by the Biden administration,[125] which **could offer a useful model** for EU action:

→ **Accountability.** Sanctions at least send a message to the victims that some accountability is being sought, and also **cause economic, operational and reputational harm** to vendors and investors which may have a deterrent effect.

→ **Corporate policy reforms:** Facing U.S. sanctions, some companies have been forced to adapt. For instance, **Sandvine**[126] restructured its operations and at least claimed to have begun "prioritising human rights con-

124. *https://www.cyberresilienceact.eu/the-cra-explained/*
125. *Politico*, "Commerce Department blacklists dozens of groups over weapons-related violations", 2024, *https://www.politico.com/news/2024/10/21/commerce-dept-blacklist-groups-00184628.POLITICO*
126. *Reuters*, "U.S. removes Sandvine from trade restriction list after corporate reforms", 2024, *https://www.reuters.com/technology/us-removes-sandvine-trade-restriction-list-after-corporate-reforms-2024-10-21/*

siderations" after being put on a prohibited list by the Bidem administration for supplying technology used in mass surveillance and censorship in Egypt. These types of reactions show that pressure via sanctions can lead to at **least some changes in vendor behaviour.**

→ **Market withdrawal from authoritarian regimes:** In some cases, sanctions have directly influenced market decisions. **Sandvine** announced its w**ithdrawal from fifty-six countries it classified as "non-democratic"**—including Egypt—stating it would restrict sales to democracies only. While this approach is imperfect (as spyware also violates human rights in democracies, and the approach also relies on the vendor's interpretation of what counts as democratic), it has still helped **produce less harm and slow down proliferation.**

→ **Deterrence:** Legal action and putting vendors on prohibited lists also serve as important deterrents. The landmark ruling in WhatsApp's lawsuit against NSO Group, where the court determined NSO had violated hacking laws, set **a precedent that may discourage similar abuses by other spyware vendors.**[127] If sanctions were also **to target investors,** this could have a crucial deterrence element for US and European capital, even if companies move abroad.

Sanctions must be part of a broader strategy to push for vendor and investor accountability and to slow down spyware proliferation. While they cannot dismantle the spyware industry on their own, they can shift incentives, limit sales, and stigmatise abusive actors - especially if adopted at EU level. **Moreover, sanctions would make it hard for EU developers to work for spyware vendors, even if they were based abroad. Importantly,, they can be adopted immediately.**

3.4 Policy recommendations to EU institutions and Member States

To address the regulatory vacuum that has allowed the commercial spyware industry to grow unchecked, the following actions are urgently required from EU institutions and Member States:

1. **Total ban on commercial spyware. The European Commission** must prohibit the development, production, marketing, sale, export, and use of commercial spyware by private companies, in line with demands from civil society organisations working in digital rights.[128]

2. **Ban on the vulnerabilities and exploits market.** The **EU Commission should enforce a ban on the commercial trade of vulnerabilities** for any purpose other than strengthening systems' security. In parallel, it should mandate the responsible disclosure of vulnerability research findings, through a uniform reporting process, and forbid outsourcing vulnerability research for offensive use by states to private, for-profit vendors.

3. **Protections for ethical cybersecurity research and responsible disclosure.** The **EU should invest in research institutions and initiatives that focus on cybersecurity** for public good, prioritising digital rights, privacy, and democratic security. **At State level, whistleblower protections** should be expanded, and governments and industry actors should establish strong incentives, such as **well-funded bug bounty programmes,** for the ethical disclosure of security flaws to developers. **Security researchers acting in good faith, and not on behalf of spyware vendors, must be free from criminal and civil liabilities** when they conduct research or when they share vulnerability information with software vendors and other security researchers.

127. *Financial Times*, "Trump's 'big, beautiful' tax bill heightens concerns over US debt", 2025, *https://www.ft.com/content/e5b770d7-07af-4e27-a686-a0c473e93770*
128. *Center for Democracy & Technology*, "Civil Society Joint Statement on the Use of Surveillance Spyware in the EU and Beyond", 2024, *https://cdt.org/insights/civil-society-joint-statement-on-the-use-of-surveillance-spyware-in-the-eu-and-beyond/*

4. **End financial incentives driving spyware proliferation. European Member States must prohibit public procurement** from commercial spyware vendors, and **ban public and private investment in spyware** companies at any level of their corporate structures.

5. **Targeted sanctions against commercial spyware actors. The High Representative of the Union for Foreign Affairs and Security Policy and the Council** should immediately agree on the following sanctions: impose **entry bans on** third-country nationals and entities involved in the commercial spyware industry, including executives and investors; **targeted visa removals** – for those already based in Europe - and travel bans for those based elsewhere; **asset freezes on both companies and individuals,**[129] including EU citizens working abroad; **put on a prohibited list those vendors** involved in any spyware scandal; and **ban exports from EU-based commercial spyware companies to any country.**

6. **Accountability for vendors, investors, and enabling states. Commercial spyware vendors must face legal consequences** for enabling human rights abuses. **Investors who knowingly fund these firms must also be held liable by competent Courts.** Similarly, **foreign states** that facilitate spyware export and deployment for repressive purposes **must face diplomatic and economic sanctions. Member States** should adapt their legislation to make this possible, **mandate their prosecutors to follow these cases,** and take steps to circumvent the opaque structures of these companies.

7. **Mandate retrospective transparency:** Commercial spyware vendors that have been operating in or from the EU, their clients, and their investors must be subject to mandatory, **retrospective public disclosure** of all their owners and shareholders, contracts, sales, and end-user agreements. **This retrospective disclosure must be required by Member State's law or through judicial mechanisms,** to fully expose the scale and scope of abuses facilitated by spyware and to guarantee effective remedy to victims of spyware up to date. These disclosures should be available **in central, searchable registries accessible to civil society organisations,** judicial authorities and lawmakers alike.

Commercial spyware vendors often rebrand, relocate, or create shell corporations to circumvent regulations. The spyware industry is sustained not only by developers but also by supporting entities: such as hosting providers, resellers, financial institutions, and consultancy firms. **All actors enabling commercial spyware development or deployment must be targeted by this regulatory action.**

129. *European Parliament,* "Enhancing research security", 2024, *https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760416/EPRS_BRI(2024)760416_EN.pdf*

4. REMEDIES FOR VICTIMS

The use of spyware has had devastating consequences for individuals, organisations, and democratic institutions. However, despite the clear violations of fundamental rights, most cases have seen a glaring absence of effective remedies for victims. This section outlines the legal and non-legal measures that must be implemented to redress injustice, ensure accountability for the harm caused and protection for affected individuals and groups.

4.1 Human Rights violations

The use of spyware raises significant concerns regarding the violation of fundamental human rights, primarily due to its intrusive and non-selective nature. As we established in Chapter 2, **its use goes far beyond, and is fundamentally incompatible with, the basic legal principles of necessity and proportionality,** which must be respected for any lawful limitation of fundamental rights, as enshrined in Article 52(1) of the Charter of Fundamental Rights of the European Union.[130]

A. Direct impact on targeted individuals

The most severe violations of fundamental human rights **occur at the level of the affected individuals – even if they were not directly targeted.** Spyware use disproportionately restricts several fundamental rights:

→ **Rights to private life and data protection.**[131] At its core, spyware directly infringes upon an individual's right to privacy and data protection. The Venice Commission[132] asserts that **the use of spyware directly impacts the right to privacy protected by international treaties.** Furthermore, the importance of the right to data protection in the EU is underscored by the dual framework of the EU,[133] which reflects a recognition that data protection is a fundamental right in its own right, central to preserving dignity, autonomy, and democratic participation. When it comes to spyware, the European Data Protection Supervisor (EDPS) has warned that **"the level of interference with the right to privacy is so severe that the individual is in fact deprived of it. In other words, the essence of the right is affected. Therefore, its use cannot be considered proportionate** – irrespective of whether the measure can be deemed necessary".[134]

130. See reference below
131. Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union; Art. 7 and 8 of the ECHR. Art 17 of the ICCPR, Art 12 of the Universal Declaration of Fundamental Rights, *European Union*, "Charter of Fundamental Rights of the European Union", 2012, *https://www.europarl.europa.eu/charter/pdf/text_en.pdf*, *United Nations*, "Universal Declaration of Human Rights", 1948, *https://www.un.org/en/about-us/universal-declaration-of-human-rights*
132. *Venice Commission*, "Report on a rule of law and human rights compliant regulation of spyware", 2024, *https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2024)043-e*
133. The General Data Protection Regulation (GDPR) for the private and public sectors, and the Law Enforcement Directive (LED) for police and criminal justice authorities
134. *European Data Protection Supervisor*, "Preliminary Remarks on Modern Spyware", 15 February 2022, pag. 8 *https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf*

→ **Right to freedom of expression, peaceful assembly and association.**[135] These rights constitute an **essential foundation of a democratic society.** As pointed out by the Council of Europe's report on the *Human Rights effects of the use of spyware*[136], "the surveillance of journalists and other media actors, and the tracking of their online activities, can endanger the legitimate exercise of freedom of expression". These rights can also be affected by the societal chilling effect of spyware (see Section B).

→ **Right to a fair trial**[137]. Spyware allows authorities to access privileged communications, potentially violating attorney-client confidentiality and undermining the fairness of legal proceedings. Lawyers of political dissidents have been targeted in many cases, such as those in Spain[138] or Jordan[139]. **In some cases, like Jordi Cuixart's**[140] **in Catalonia, victims were targeted while preparing the strategy for their trial,** which raises concerns about the validity of the process due to a violation of the right to defence.

→ **Right to equality and non discrimination**[141]. Women, LGBTIQ+ and gender-diverse communities experience unique gendered fears upon discovering their digital privacy had been infringed, such as the use of their data to facilitate online harassment, especially 'doxing'.[142 & 143]

B. Indirect impact on non-targeted individuals and communities

Human rights violations caused by spyware are not confined to a single dimension; rather, they unfold on multiple levels. Indirectly, they manifest across three levels of impact:

1. Impact on persons connected with targeted individuals

Spyware also infringes the privacy of others connected to the targeted individuals. This includes 'collateral damage' to confidential sources, attorneys, colleagues, family members, and children, whose personal data or communications may also be unlawfully accessed.[144]

2. Societal impact through the chilling effect

The use of spyware **can also create a chilling effect,**[145] indirectly undermining other fundamental rights such as freedom of expression, freedom of association and assembly, the right to a fair trial, and others. **When individuals suspect they are being monitored, or know they are, they may be less likely to speak out, share dissenting opinions, organise protests,** or participate in civic activities, effectively silencing themselves out of fear of retaliation or exposure. In this way, spyware not only infringes on individual rights but also **weakens collective democratic participation.** It can also have severe **mental health impacts,** such as insomnia, nightmares, and psychological trauma, in some cases resulting in the need for herapy or withdrawal from activism.[146] This disengagement from activism or self-censorship has grave effects in the civic space.

3. Impact on those on whom it is tested or through whom is developed

Furthermore, spyware abuses extend along **the value chain**: spyware companies, investors, and exporting states all play a role in perpetuating these human rights violations from its development through to its deployment by the buying authorities. A clear example is the **case of Israel, the leading exporter of commercial spyware and digital forensics tools.** It has been consistently reported that many of the commercial spyware tools created in and exported from Israel have been tested on Palestinians[147 & 148] before being marketed. Even with companies moving out from Israel to set up shop in the EU, it has been documented that **56 out of 74**

135. Art 11 Charter, Art. 10 ECHR
136. *Council of Europe*, "Pegasus Spyware and Its Impacts on Human Rights", 2022, *https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8*
137. Art. 47 Charter, Art. 6 ECHR
138. *TechCrunch*, "Lawyer allegedly hacked with spyware names NSO founders in lawsuit", 13 November 2024, *https://techcrunch.com/2024/11/13/lawyer-allegedly-hacked-with-spyware-names-nso-founders-in-lawsuit/*
139. *Security Week*, "At Least 30 Journalists, Lawyers and Activists Hacked With Pegasus in Jordan, Forensic Probe Finds", February 2024 *https://www.securityweek.com/at-least-30-journalists-lawyers-and-activists-hacked-with-pegasus-in-jordan-forensic-probe-finds/*
140. *Front Line Defenders*, "Jordi Cuixart released from prison on pardon", 2021, *https://www.frontlinedefenders.org/en/case/jordi-cuixart-released-prison-pardon*
141. Arts. 20 and 21 Charter, Art 14 ECHR
142. *Amnesty International*, "Being ourselves is too dangerous: Digital violence and the silencing of women and LGBTI activists in Thailand", 2024, *https://www.amnesty.org/en/wp-content/uploads/2024/05/ASA3979552024ENGLISH.pdf*
143. Other rights potentially affected by the use of spyware, as protected by the EU Charter of Fundamental Rights, include the principle of human dignity (Art. 1), the right to liberty and security (Art. 6), freedom of thought, conscience, and religion (Art. 10), the right to engage in collective bargaining and collective action (Art. 28), when workers and their organisations are targeted, and the presumption of innocence and rights of the defence (Art. 48), as information is gathered prospectively, and control over devices can be used to fabricate false evidence.
144. *Conseil Constitutionnel France, Ibidem.*
145. *Amnesty International, Ibidem.*
146. That is the case, for example, of activist Pansiree Jirathakoone, targeted by Pegasus by the Thailand Government. *Amnesty International, Ibidem.*
147. *Chatham House*, "Review: Why Israel tests its spyware on Palestinians", 2023, *https://www.chathamhouse.org/publications/the-world-today/2023-06/review-why-israel-tests-its-spyware-palestinians*
148. *Foreign Policy*, "How the Occupation Fuels Tel Aviv's Booming AI Sector", 2022, *https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/*

governments[149] investigated in a report are procuring surveillance technologies from firms **connected to the country.** Companies are either based in Israel (such as **NSO Group, Cellebrite, Cytrox,** and **Candiru)**, or they have among their top executives former **Israeli Defence Forces (IDF)**[150] staff bringing the technical expertise, as in the case of **Intellexa**.[151]

4.2 Remedies

The **absence of effective remedies in Europe has left victims without recourse, reinforcing impunity for spyware vendors and users.** A robust framework of legal and non-legal remedies must be established to provide justice, accountability, and support for affected individuals and communities.

A. Legal remedies

The state, often the deployer of spyware, **is unlikely to provide impartial legal remedies,** and victims of spyware face substantial obstacles to obtaining justice. However, EU countries are obligated to comply with the **right to effective remedy**[154]**, which has, according to International Human Rights Law (IHRL), three main components**[155]**:**

→ Access to relevant information concerning violations and reparation mechanisms

→ Equal and effective access to justice; and

→ Adequate, effective and prompt reparation for harm suffered

Therefore, the following are the minimum legal remedies that the **EU Member States** must guarantee, ex post, for victims of spyware to uphold human rights law.

1. Right to know: transparency and access to information. Victims must **have full access to detailed information about spyware operations,** including **who** deployed the spyware against them, the judicial authority that authorised its use, and the **legal basis.** This remedy also extends to **transparency regarding the spyware vendors**, as mentioned in Chapter 3.

2. Right to data protection and information on data storage: Individuals should know precisely **the scope of the interference** with both their historical and real-time data. This includes **which personal data** were seen, monitored or extracted; **when**; by **whom (with an exhaustive log)**; **where the data are stored**; and **how they are protected.** It also encompasses understanding the security measures in place, the protocols for data retention and deletion, and any instances where data may have been intercepted or manipulated.

3. Right to accountability and judicial redress: There must **be clear, accessible judicial pathways** that allow victims to **hold both state actors and private companies accountable.** Legal proceedings should **clarify the applicable jurisdiction,** ensure proper oversight, and impose sanctions on those responsible, with **prosecutors actively pursuing prosecutions.**

149. *Carnegie Endowment for International Peace,* "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses", 2023, *https://carnegieendowment.org/research/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229*
150. The IDF have been the main actor in developing practices which, according to the UN, are "consistent with the characteristics of genocide" in the Gaza Strip, in the context of the 2023-2025 war. *United Nations General Assembly,* "Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories", 2024, *https://docs.un.org/en/A/79/363*
151. Founded in 2019 by former Israeli military officer Tal Jonathan Dilian, Intellexa has emerged as a key player in the global market for commercial spyware. *Turkiye Today,* "US imposes sanctions on Greece-based company founded by ex-Israeli military officer", 2024, *https://www.turkiyetoday.com/world/us-imposes-sanctions-on-greece-based-company-founded-by-ex-israeli-military-officer-8398/*
154. Art 47 Charter, art 13 ECHR.
155. *Amnesty International, Ibidem.*

4. Right to an independent investigation: As the European Parliament's inquiry committee on Pegasus and equivalent surveillance spyware[156] has demanded, victims should be entitled to an **impartial, independent investigation into alleged spyware abuses.** Such investigations must have the authority to **collect evidence** – even if protected by secrecy legislation -, **question relevant parties,** including government officials, company staff and investors, and operate free from political or commercial interference, thereby ensuring that **the truth is fully uncovered.**

5. Right to compensation: Compensation must address not only financial losses but also non-**monetary harms such as effects on mental health.** This form of redress serves both as a **remedy** for the individual and as a **deterrent** to future use of spyware technologies.

6. Right to non-repetition: Legal frameworks must enforce **systemic reforms to prevent future violations** by state authorities or others, and so that jurisprudence evolves to prevent future human rights violations.

While these remedies remedies are essential to uphold victims' rights in the face of spyware abuses, they are stop-gap measures that cannot substitute the primary objective: the full prohibition of spyware in line with fundamental rights obligations.

B. Non-legal remedies

In addition, EU Member States must ensure **the following non-legal remedies** are applied by public administrations in relation to victims of spyware:

1. Psychological support: Providing free and independent **mental health resources** and support to victims who have experienced trauma due to surveillance and repression.[157]

2. Consideration for asylum-seekers and undocumented people: Supporting victims whose **safety has been compromised by spyware,** and who must seek refuge elsewhere, by providing them with asylum and protection.

3. Facilitate access to victim support. Launch public information campaigns focused on spyware risks, digital self-defence, and help pathways (for example, helplines, legal aid, and civil society support). **Ensure affected individuals know their rights** and where to turn for support.

4.3 The role of strategic litigation in combating spyware abuses

Judicial decisions are indispensable for establishing robust frameworks against the use of spyware, as courts often represent the last bastion for upholding human rights protections. Strategic litigation provides multiple avenues for accountability: challenging legal provisions that permit spyware use, exposing instances where governments use spyware, and initiating proceedings against companies.

156. Website: *https://www.europarl.europa.eu/committees/en/archives/9/pega/home/welcome-words*
157. *Forbes Technology Council*, "Recognizing and Preventing the Psychological Toll of Spyware", 2022, *https://www.forbes.com/councils/forbestechcouncil/2022/08/12/recognizing-and-preventing-the-psychological-toll-of-spyware/*

A notable example is the **FinFisher case in Germany.** Following a criminal complaint submitted by organisations such as the **Gesellschaft für Freiheitsrechte e.V., Reporters Without Borders (RSF), the European Centre for Constitutional and Human Rights (ECCHR),** and netzpolitik.org, the Munich Public Prosecutor's Office seized the assets of the FinFisher group[158]. **Consequently, FinFisher GmbH and its partner companies filed for insolvency.** Another example is the Federal Constitutional Court's establishment of high standards for the use of state-built spyware ("statetrojaner") in a judgement in 2008[159] . These cases demonstrate how strategic litigation can serve as an effective lever to combat spyware abuse.

But on their way to achieving justice and change, victims across Europe are encountering similar obstacles: .

→ **Secrecy and withholding of information:** Governments often invoke secrecy laws that prevent critical information from reaching the public, like in the Greek case[160] and in Germany, concerning the reports of the use of Pegasus by the Federal Criminal Police Office (BKA);

→ **Prosecutorial inaction:** This inaction by the state – often the same actor responsible for the illegal surveillance - not only forces victims to expend significant resources, time, and emotional labour, but can result in **secondary victimisation - whereby the state's failure to act deepens the harm suffered.** This is, for example, **the case in Catalonia,** where four years after Catalan civil society, lawyers and politicians were found to have been hacked by Spanish authorities in the Catalangate scandal[161], **public prosecutors in Spain have systematically blocked all judicial cases;**[162]

→ **Jurisdictional complexities:** The global nature of spyware vendors adds another layer of difficulty. With companies headquartered in one country and operating subsidiaries in another (e.g. an Israeli-based company with subsidiaries in Luxembourg[163]) and victims in a third one, establishing clear jurisdiction becomes problematic. **As a result, many courts decline to take on cases, citing jurisdictional limitations.** And even when courts accept cases, it remains highly difficult to enforce decisions against companies which are not based in the EU.

Another barrier is that there is currently a lack of European case law concerning spyware use. If the ECtHR and the European Court of Justice uphold **their strong commitment to human rights protection,** when spyware cases reach their dockets, these courts can provide **essential judicial backing to ensure that remedies and accountability are upheld when it comes to state-use of spyware.**

4.4 Protection of civil society organisations handling spyware cases

Civil society organisations and investigative journalists working on spyware detection, digital forensics and incident response are often the only actors exposing state use of spyware, and therefore must be adequately shielded from legal intimidation and potential state-imposed consequences. These organisations offer their services and protection to journalists, activists, members of civil society and unjust targets of state repression because of the work they do. The ability of civil society organisations to function effectively is severely restricted in authoritarian and hybrid regimes, where authorities act outside the law and prioritise the interests of the ruling parties over those of the people, but increasingly also in countries formally considered democratic.

They are not only directly targeted by state authorities, but also face additional threats, including blackmail, intimidation, and personal attacks in the media. As seen in the Serbian case[164], these organisations and their employees are sub-

158. *Netzpolitik,* "German Made State Malware Company FinFisher Raided", 2020, *https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/*
159. *Bundesverfassungsgericht,* "Urteil vom 27. Februar 2008 – 1 BvR 370/07", 2008, *https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html*
160. *Politico,* "Greece leaves spy services unchecked on Predator hacks" , 2024 ,*https://www.politico.eu/article/greek-spyware-predatorgate-government-court-report-telephone/*
161. *The Citizen Lab,* "CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru", 2022, *https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/*
162. *Politico,* " Catalonia reignites its court fight with Spain over spyware ", 2025, *https://www.politico.eu/article/catalonia-reignite-court-fight-spain-israel-pegasus-candiru-spyware-hacking/*
163. This is the case with NSO Group, which Catalan organisation Iridia has been able to indict after three years of legal struggle. *Iridia,* "Three executives of the NSO Group charged for their responsibility in the Pegasus espionage case", 2025, *https://iridia.cat/en/three-executives-of-the-nso-group-charged-for-their-responsibility-in-the-pegasus-espionage-case/*
164. A good example is the smear campaing of the Serbian government against SHARE Foundation, who helped uncovering the Serbian spyware scandal. This news reads: "Share Foundation receives more than €4 million: They invented a story about spying on journalists, and they are funded by Switzerland" – which is totally invented. Novosti RS "SHARE FONDACIJA DOBILA VIŠE OD ČETIRI MILIONA EVRA: Izmislili priču o špijunaži novinara, a finansira ih Švajcarska", December 2024 *https://www.novosti.rs/vesti/politika/1444129/share-fondacija-dobila-vise-cetiri-miliona-evra-izmislili-pricu-spijunazi-novinara-finansira-svajcarska*

jected to smear campaigns and disinformation efforts - often orchestrated by tabloids with close ties to the government. Furthermore, attempts to discredit both the organisations and their staff further undermines their work, creating a climate of fear and hostility that hinders their efforts to expose and address the abuses they are investigating. Additionally, another strategy to discredit them is state authorities requesting access to victims' devices – the same authorities that abused them. This practice should be discouraged, and civil society or other independent third-party forensics experts recognised and legitimised to do those analysis instead of state authorities.

These civil society organisations, together with journalists, are usually the only actors who can uncover cases of spyware-related human rights violations and therefore often represent the only effective remedy available to targeted individuals. **As a result, it is of utmost importance that independent national and international bodies** — including national ombudspersons, national data protection officers, European Union institutions, the Council of Europe, and the United Nations — **timely and decisively react to any malicious targeting of civil society organisations handling spyware cases.** This is even more urgent in the context of wider efforts, usually from far-right actors, across Europe and the world to attack, scapegoat and delegitimise civil society and democratic counter-speech.

4.5 Recommendations to the European Union institutions and Member States

To address the real-world impact of spyware and provide meaningful remedies, ensuring that everyone involved in human rights abuses is held liable, the following measures must be implemented:

1. Full access to legal and non-legal remedies for all victims

→ **Member States** must ensure that all legal and non-legal remedies outlined in this chapter are accessible to any individual affected by spyware, regardless of nationality or status. This includes:

→ **Legal remedies:** the right to know, the right to data protection and information on storage, judicial redress, independent investigation, compensation, and guarantees of non-repetition.

→ **Non-legal remedies:** psychological support, protection mechanisms for asylum seekers, public awareness campaigns, and facilitated access to victim support.

2. Remove judicial barriers for existing victims

→ **The Council of the European Union and Member States must mandate binding obligations for prosecutors to investigate spyware complaints** by victims, remove discretionary inaction, and ensure support for courts with **specialised units or independent investigators equipped to handle such complex cases.**

→ **Member States must establish adequately resourced independent investigative bodies** to examine spyware abuse cases beyond political influence, and **to avoid victims having to turn over their devices** to authorities they might not trust.

→ **Guarantee support for victims already entangled in lengthy, obstructed or stalled legal proceedings,** including expedited review, procedural support, and access to digital forensics assistance and reform jurisdictional rules to allow EU-based victims to bring transnational spyware cases, especially where vendors operate across multiple states.

3. Ensure political accountability and structural reform

→ **The European Commission** must implement the **enforcement of the PEGA Committee recommendations.** It should particularly urge EU Member States to **conduct immediate, independent, transparent, and impartial investigations of any cases of unlawful surveillance,** if needed with the impulse of their State prosecutors, under the threat of application of the Rule of Law mechanism or infringement procedures it is not enforced;

→ **The European Commission should require Member States** to provide **full transparency in public procurement and deployment** of spyware tools by Member States, **including mandatory public reporting on spyware use.**

→ **Member States** affected by scandals should convene Parliamentary Inquiry Committees with enough powers to assess the scale, cost, and legal grounds of state use of spyware, as well as public procurement details.

→ **Member States** should also **reform secrecy laws that shield unlawful surveillance data** – basic for the victims' right to know - behind "secrecy" justifications, particularly when used to deny remedies to victims.

4. Protect HRDs, journalists, lawyers and CSOs

→ The European Commission must develop and fund an **EU-wide emergency protection mechanism**[165] for journalists, human rights defenders (HRDs), lawyers, and whistleblowers under spyware threat in the EU and beyond. This mechanism should offer:

→ Preventive digital security support, including device security checks, communications training, and real-time spyware detection.

→ **Independent forensic assistance** and trusted helplines for at-risk individuals.

→ **Emergency relocation,** legal aid, and financial support for those in imminent danger.

→ The European Commission should also establish an E**U fund for civil society organisations and individuals such as journalists engaged in spyware detection,** forensics, and victim support, including an emergency fund accessible in both Member States and EU candidate countries, to support them operationally.

→ **Member States must go beyond the European Media Freedom Act (EMFA) by explicitly prohibiting spyware** use on anyone (including journalists, lawyers and human rights defenders), and also guaranteeing access to rapid-response protection and redress mechanisms for those already targeted. These measures should complement victims' rights outlined in Recommendations 1 and 2.

→ In parallel, **Member States must urgently transpose and implement the Anti-SLAPP Directive effectively, and adopt ambitious judicial and non-judicial measures to better protect individuals and CSOs from SLAPPs.** This includes integrating provisions from related non-binding texts, such as the **2022 European Commission Anti-SLAPP Recommendation and the Council of Europe's 2024 Recommendation,** as well as provide public funding for CSOs involved in forensics and victim support.

165. A good model would be the protectdefenders.eu initiative, protecting human rights defenders at risk with EU funding, but coordinated by specialised CSOs.

5. GLOSSARY

→ **Attack vector:** a method or "way" used to deliver spyware to a target, such as malicious links, deceptive ads, physical access or a particular vulnerability.

→ **Brute force:** A method of circumventing security protections by systematically and automatically attempting all possible combinations of credentials, passwords, access codes, or other authentication factors until access to the device is gained.

→ **Bug bounty:** a bug bounty programme is a deal offered by websites, organisations, governments and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

→ **Commercial spyware vendors:** private companies that develop and provide offensive cyber capabilities (enabling disruption or surveillance) for profit. They are also referred to as "commercial surveillance vendors" or "cyber mercenary firms", which may offer a variety of surveillance technologies including (or not) spyware. Hence we use the specific term of "commercial spyware vendors" for the purpose of this paper in order to designate those among the industry that sell spyware as a commercial product.

→ **Exploit:** a segment of code or a program that maliciously takes advantage of vulnerabilities or security flaws in software, often used to install spyware.

→ **Intrusion-as-a-Service:** a commercial model in which private actors sell intrusion capabilities - including spyware - on demand.

→ **Logging:** the process of recording any activity on a device. Spyware often disables or avoids logs to make its presence and use undetectable.

→ **Mandated encryption backdoor:** a deliberately inserted vulnerability that allows third-party access to encrypted data - undermining trust and security for all users.

→ **Remote access:** the capability to monitor or control a device from afar, without direct physical contact with the device.

→ **Telemetry:** data collected by software or systems - such as location or usage stats - often repurposed for surveillance without clear user consent.

→ **Vulnerability:** a software vulnerability is a structural or design flaw present in a software application that can be exploited by attackers to compromise the security and functionality of the system, network or data with which it interacts.

→ **Zero-days:** security vulnerabilities that hackers can use to attack systems. The term "zero-day" refers to the fact that the vendor or developer is not yet aware of the flaw and therefore had "zero days" to fix it.

EDRi
European Digital Rights