STUDY

Requested by the PEGA Committee

European Parliament

The impact of Pegasus on fundamental rights and democratic processes

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 740.514 - January 2023

EN

The impact of Pegasus on fundamental rights and democratic processes

Abstract

This study - commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA) - analyses the impact of the use of Pegasus and similar spyware on Article 2 TEU values, on privacy and data protection, and on democratic processes in Member States.

This document was requested by the European Parliament's Committee of Inquiry to investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA).

AUTHORS
Prof. Dr Giovanni SARTOR, University of Bologna and European University Institute,
Prof. Dr Andrea LOREGGIA, University of Brescia

ADMINISTRATOR RESPONSIBLE
Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT
Ivana KLECAN

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: mailto:poldep-citizens@europarl.europa.eu

Manuscript completed in December 2022

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

CONTENTS

LIST OF ABBREVIATIONS 5

LIST OF FIGURES 6

EXECUTIVE SUMMARY 7

1. GENERAL INFORMATION 10

2. MALWARE, VULNERABILITIES AND THREATS 11

2.1. Malicious software 12

2.2. Vulnerabilities 13

2.3. New threats 15

3. PEGASUS AS A SURVEILLANCE TOOL 19

3.1. Traditional and new surveillance 19

3.2. The challenge posed by spyware 21

3.3. Critical features of Pegasus 22

3.3.1. Complete access 22

3.3.2. Zero-click attacks 23

3.3.3. No (or few) traces 24

3.3.4. A multi-layered open environment 25

3.3.5. Content manipulation 25

3.3.6. The use of Pegasus 25

4. PEGASUS AND (DELIBERATIVE) DEMOCRACY 27

4.1. The idea of participatory-deliberative democracy 28

4.2. The impact of pervasive surveillance on democracy 29

4.3. Some evidence of interference in democratic processes through Pegasus 32

5. NATIONAL SECURITY: JUSTIFICATION OR PRETENCE? 34

5.1. The concept of national security 34

5.2. National security as a real or purported justification 36

6. PEGASUS AND INTERNATIONAL HUMAN RIGHTS LAW 39

6.1. The UN framework 39

6.2. The framework of the European Convention on Human Rights 42

7. PEGASUS AND EU LAW 45

7.1. Spyware and national security in the EU Treaties 45

7.2. The Court of Justice on fundamental rights, data protection, and national security 48

7.3. National security and data protection in EU law 49

7.4. The use of spyware for the purpose of law enforcement 52

8. THE WAY FORWARD 54

8.1. Lawful restrictions of fundamental rights for national security purposes 55

8.2. The use of spyware in the framework of EU law 55

8.3. What about Pegasus? 58

REFERENCES 61

LIST OF ABBREVIATIONS

AGRI	Agriculture and Rural Development Committee
ALDE	Alliance of Liberals and Democrats for Europe
BAS	Brake-assist systems
CAP	Common Agricultural Policy
CFP	Common Fisheries Policy
CMO	Common market organisation
CoR	Committee of the Regions
CULT	Culture and Education Committee
ECOSOC	Economic and Social Committee
ECR	European Conservatives and Reformists
ECTS	European Credit Transfer System
EFDD	Europe of Freedom and Direct Democracy Group
ENF	Europe of Nations and Freedom
EPP	Group of the European People's Party (Christian Democrats)
FAO	Food and Agriculture Organisation of the United Nations
FPS	Frontal protection systems
GDP	Gross Domestic Product
GM	Genetically-modified
Greens/EFA	The Greens/European Free Alliance
GUE/NGL	European United Left - Nordic Green Left
IFI	International Fund for Ireland
S&D	Group of the Progressive Alliance of Socialists and Democrats in the European Parliament

LIST OF FIGURES

Figure 1: Malware taxonomy 12
Figure 2: Diagram of web-malware spread mechanism 15
Figure 3: Cybersecurity Threats 16
Figure 4: Top ten detection categories in 2021 17
Figure 5: Stages of surveillance and the seven entities identified by Meta 18
Figure 6: Data collection through Pegasus 23
Figure 7: Installation of the Pegasus agent 24
Figure 8: The Pegasus data-collection process 25
Figure 9: Who has been targeted by Pegasus 38

EXECUTIVE SUMMARY

Background

Targeted surveillance based on technological tools raises justified concerns owing to its depth, as it can extend across all life aspects of the targeted individuals. Spyware systems that hack mobile devices - as with Pegasus, developed by the Israeli NSO Group - enable pervasive secret surveillance. Pegasus has full and unrestricted access to the hacked device: it can extract all the data in it (initial data extraction), monitor all activities performed through it (passive monitoring), activate the device's functionalities to collect further data (active monitoring), and possibly interfere with the content in the device and the messages sent by it (manipulation). It can be installed without any action by the individuals concerned and will leave no trace of its operation (or at least very few traces).

Aim

The aim of this report is to (a) identify key issues concerning the ways in which Pegasus and other spyware may interfere with individual rights and democratic processes and institutions, (b) assess the relevant legal framework, (c) determine the extent to which and the conditions under which spyware may be lawfully used, and (d) recommend ways to implement such conditions.

Impact on rights and democracy

Pervasive surveillance affects people's privacy, data protection, and further individual rights —such as the rights to freedom of speech, association, and assembly— as well as the democratic institutions of society. Political participation is affected by spyware in that spied-on citizens can feel compelled to abstain from engaging in interactions having political content, from sincerely expressing their views, and from associating with others for political purposes. This impinges on the quality of a democratic public sphere, which ultimately relies on citizens' input and reactions. More specifically, spyware affects individuals (like journalists, politicians, and activists) who play a special role in the public sphere. Surveillance of such individuals opens space for repression, manipulation, blackmailing, falsification, and defamation. The electoral process itself may be influenced, where the collected information, possibly manipulated, is used to carry out smear campaigns against targeted candidates or to engage in other actions affecting their chances of success in the elections. The mere fear of being spied on may induce people to refrain from running for office or from running an effective campaign.

Spyware and national security

The use of spyware is usually justified by invoking national security or law enforcement purposes. However, it appears that in many cases spyware is used for other purposes, often pertaining to partisan political objectives or to the repression of social and political dissent. It has been recognised that many states have used national security as a cynical legal pretext to curtail freedom of expression, legitimise torture and other ill-treatment, and exert a chilling effect on minorities, activists, and political opposition. In particular, extensive evidence exists on Pegasus being used to target individuals not having any connection to serious crimes or national security threats, such as political opponents, human rights activists, lawyers, and journalists. To prevent an expansive use of the notion of *national* security, this notion should be understood restrictively and distinguished from the concept of *internal* security, the latter having a broader scope, including the prevention of risks to individual citizens, and in particular the enforcement of criminal law.

International human rights law

In the UN framework, surveillance activities are to be assessed according to human rights treaties such as the International Covenant on Civil and Political Rights. Abusive surveillance affects not only the right to privacy but also freedom of expression and other rights in the Covenant. Both privacy and freedom of expression can only be limited through the law and as necessary for legitimate purposes. National security may justify limitation, but in the case of Pegasus, the legality and necessity requirements are likely not satisfied.

According to the European Convention on Human Rights, the requirements of legitimacy, legality, necessity, and proportionality, in the context of a democratic society, apply to all instances of targeted surveillance. An extensive case law of the European Court of Human Rights (ECtHR) has set conditions for covert surveillance to be consistent with human rights, particularly with regard to legality (accessibility of the laws authorising surveillance and foreseeability of their consequences) and notification. The Court has also granted standing to individuals even only potentially affected by covert surveillance.

EU law

In the context of EU law, targeted surveillance is relevant to the rights contained in the Charter of Fundamental Rights of the European Union, to the principles contained in the Treaties (such as democracy and the rule of law), and to various instruments of EU secondary law, such as those pertaining to data protection.

According to the Treaty on European Union (TEU), national security is the sole responsibility of each Member State, but this does not in principle exclude that national security activities are subject to EU law, which indeed is the case when they interfere with activities regulated by EU law.

The application of EU law to the use of spyware for national security purposes is, however, hindered by the exclusion of national security from the scope of two fundamental instruments: the GDPR and the ePrivacy Directive. This can hardly be justified with regard to the rights enshrined in the Charter and the principles contained in the Treaties. Because this exclusion may be used too broadly, it must be pointed out that it only concerns cases in which the spyware is genuinely used to protect national security properly understood. EU law fully applies to the use of covert investigations for law enforcement purposes. However, even in this domain, there is evidence of abuse.

Recommendations

The use of spyware poses a threat to the fundamental rights and basic principles of EU law, such as (representative-deliberative) democracy and the rule of law. It risks undercutting the very principles on which the EU legal system is based.

In the international and European legal systems, national security activities can justify restrictions on fundamental rights, but if such restrictions are to be lawful, they need to satisfy the conditions of *legitimacy*, *legality*, *necessity*, *balancing*, and *consistency with democracy*.

In many instances of its deployment, Pegasus has so far failed to meet these requirements, given that it has been used for non-legitimate purposes, without an adequate legal framework, in the absence of real necessity, causing disproportionate harm to individual rights, and undermining democracy.

We suggest various strategies that may help prevent abuses:

- Circumscribing the material scope of national security activities so as to make it more difficult for states to use national security as a spurious legal justification for activities directed at other purposes.

- Circumscribing the personal scope of national security activities, excluding from it certain activities by private parties.
- Including national security activity within the scope of data protection law, so as to ensure that restrictions of data subject rights for national security purposes are subject to requirements of legality and proportionality.
- Supporting the adoption of adequate legal frameworks at the national level, since national security remains a reserved competence of Member States, and it is up to them to effectively ensure that their activity complies with the fundamental rights and principles of EU law. These frameworks should comply with principles such as the following: legality, legitimate end, necessity, proportionality, competent authority, due process, user notification, transparency, public oversight, security and certification, and technical adjustability.

A politically feasible moratorium on the use of device-hacking tools could consist in a strong presumption against the lawfulness of their use, a presumption grounded in extensive evidence of their abusive deployment. This presumption could only be overcome when a state convincingly shows a willingness and capacity to prevent all abuses.

Moreover, all Member States should be urged to ban the use of specific spyware tools where, as with Pegasus, there is strong evidence of their extensive deployment in unlawful activities, especially within the EU. Until there is clear evidence that such unacceptable practices no longer take place, continuing to deploy Pegasus, even in the framework of lawful activities, amounts to supporting its producers and developers and thus implies a political (even if not a legal) complicity with such practices.

1. GENERAL INFORMATION

We examine the extent to which human rights law and EU law can be applied to the deployment of spyware for alleged national security purposes. After introducing the various kinds of malevolent attacks to digital devices (Section 2), we focus on systems which operate by hacking mobile devices, as is the case with Pegasus (Section 3). We discuss the impacts of Pegasus on democracy (Section 4), and the appeal to national security as a justification for covert surveillance (Section 5). We will consider the applicable legal framework: human rights instruments, such as the International Covenant on Civil and Political Rights and the European Convention on Human Rights (Section 6), and EU law, including the EU Treaties, the EU Charter of Fundamental Rights, and data protection instruments (Section 7). Finally, we offer some considerations on whether and under what conditions spyware may be lawfully deployed (Section 8).

2. MALWARE, VULNERABILITIES AND THREATS

KEY FINDINGS

Technological devices represent our interface to the digital world. This is a growing network of devices that are connected to the Internet and can communicate with each other and with humans. We use these devices to store information and communicate; they have sensors or other technology built into them that allow them to collect data from the physical environment. Spyware enables intruders to access and use digital devices without knowledge or consent by the legitimate users. The data being collected, including sensitive information, can be used in ways that are not in line with users' expectations or preferences. Various kinds of malicious software tools exist that exploit vulnerabilities to engage in unauthorised activities.

There are many potential reasons why third parties might be interested in gaining unauthorized access to a device or a group of devices. Some of the possible goals are as follows:

- Collecting information about the target (the user of the device). This might include personal data such as name, address, and phone number, as well as information about the target's online activities and habits.
- Collecting information about the target's acquaintances. This might include data about the people the target communicates with, as well as information about their online activities and habits.
- Gaining access to the device with the goal of asking for a ransom. In this case, the third party might try to take control of a device and make its content inaccessible (by encrypting it) and then demand a payment from the owner in exchange for returning control of the device to the user and enabling access the data.
- Identity theft. If a third-party gains access to a device, they may be able to impersonate the owner of the device and send messages or perform other actions that appear to be coming from the legitimate owner. This can be especially dangerous if the third party is able to gain access to sensitive personal or financial information through the device.
- Making the target unable to use the device. This might be done by deleting important files or disabling key functions of the device.

Various technologies may be used to carry out cyberattacks.[1] By understanding the technologies that attackers may use, individuals and organizations can take steps to protect themselves and their systems. The following approaches are most significant:

- Malware.[2] This term is short for *malicious software*. The malware is intended to attack a standalone computer or a connected PC, for purposes such as information or identity theft, espionage, and interruption of services.
- Phishing.[3] This online scam involves tricking users into revealing sensitive information, such as passwords, account numbers, or personal data. This information can then be used for nefarious purposes, such as stealing money from a user's bank account or using the information to gain

[1] Saeed, I.A., Selamat, A. and Abuagoub, A.M.. "A survey on malware and malware detection systems."

[2] Saeed, I.A., Selamat, A. and Abuagoub, A.M. "A survey on malware and malware detection systems." *International Journal of Computer Applications* (2013), 67(16).

[3] Kathrine, G.J.W., Praise, P.M., Rose, A.A. and Kalaivani, E.C. "Variants of phishing attacks and their detection techniques." In *3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2019, pp. 255-259.

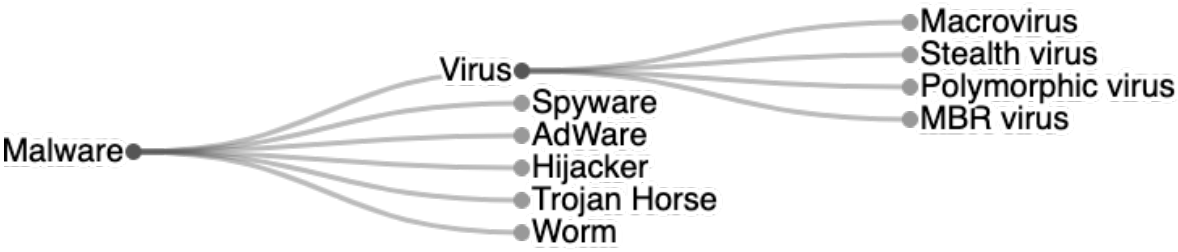
unauthorized access to a user's accounts or devices. Phishing attacks often involve the use of fake websites or emails, designed to trick users into giving away sensitive information.

- Clickjacking.[4] This attack involves tricking online users into clicking on a fake hyperlink or button, designed to deceive users. When users clicks on the link, they may be routed to a different website, a fraudulent app may be downloaded, or confidential data may be exposed. These attacks can be used to steal personal information, install malware on a user's device, or perform other adverse actions.
- Social engineering.[5] This attack involves manipulating people in order to gain access to sensitive information or systems. Social engineering use various tactics, such as phishing emails, phone calls, or in-person interactions. The attacker may pretend to be someone that the victim trusts, such as a colleague, a customer service representative, or a member of a financial institution, in order to gain the victim's confidence and coax them into divulging sensitive information or taking other actions that compromise their security.

2.1. Malicious software

As noted above, malware attacks involve the use of malicious software.

Figure 1: Malware taxonomy



Different kinds of malicious software exist, as shown in Figure 1.

- Viruses can replicate themselves and spread to other computers. They are often transmitted through infected files or emails, and can cause a variety of problems, including slowing down a computer's performance, deleting important files, or stealing personal information. They can take different forms and be developed in different programming languages. Some examples are as follows:
    - Macro-viruses. They are written using macro programming languages such as Visual Basic for Applications (VBA). Macros are a way to automate and simplify tasks in software such as Microsoft Office, and they can be stored as part of a document or spreadsheet. Macro viruses spread when infected documents or files are shared with others. When a user opens an infected file and enables macros, the virus execute itself causing harm to the user's device or data, or stealing sensitive information.
    - Stealth viruses. They have the capacity to hide from operating system or anti-virus software by making changes to file sizes or directory structure. Stealth viruses are anti-heuristic, i.e., they are designed in such a way that their detection is difficult.

[4] Sahani, R. and Randhawa, S. "Clickjacking: Beware of Clicking. *Wireless Personal Communications* (2021), 121(4), pp.2845-2855.

[5] Salahdine, F. and Kaabouch, N., Social engineering attacks: A survey. *Future Internet* (2019), 11(4), p.89.

  - Polymorphic viruses. They are designed to change their appearance and code every time they infect a different system. This can help them to evade detection by anti-virus software.
  - Boot Sector Viruses. They infect the first sector of the hard drive in the attacked computer, where the Master Boot Record (MBR) is stored. The Master Boot Record contains the disk's primary partition table and the bootstrapping instructions which are executed as soon as the computer is started.[6] When a computer infected with a Boot Sector Virus is turned on, the virus launches immediately and is loaded into memory, enabling it to control the system.

- Spyware is designed to gather information about users without their knowledge or consent. It can track users' online activities, steal personal information, or display unwanted advertisements. Spyware can be spread through infected files or emails, or it can be bundled with other software and installed without the user's knowledge. It can also download other malicious programs from the Internet and install them on the device.
- Adware displays unwanted ads. It can be automatically installed on a device, without knowledge of its user, when the user activates a program or accesses a website carrying the adware. The adware usually presents ads through pop-up windows or through bars on the screen, and may collect and transmit information about the user.
- Trojan horses are disguised as legitimate programs or files. Unlike viruses, they cannot replicate themselves and spread to other computers. Trojan horses often open a "backdoor" into a device, which allows attackers or malicious programs to gain access to the system. Thus, they can be used to steal confidential and personal information, or to perform other unauthorised actions.
- Worms are designed to replicate themselves and spread over computer network, often without the users' knowledge. They do not attach themselves to existing programs like viruses do, and they do not typically damage data or programs. However, they consume resources and spread to other devices. They slow down network performance or consume bandwidth.

2.2. Vulnerabilities

Vulnerabilities are weaknesses or flaws in a system or device that can be exploited by attackers to gain unauthorized access or perform other malicious actions. These vulnerabilities can be present in the operating system, in software applications, or in the hardware itself, and they can allow attackers to interfere with the normal operation of a device or IT infrastructure.

Vulnerabilities can be discovered by security researchers or by attackers. They can be exploited through various methods, such as malware, phishing attacks, or special "exploits" (software programs, chunks of data, or sequences of commands that are meant to take advantage of the vulnerability). By exploiting vulnerabilities, attackers can gain access to sensitive information, disrupt the normal operation of a device or system, or perform other adverse actions.

[6] Immediately after the execution of the Basic Input-Output System (BIOS), the firmware that initialises the computer hardware.

A zero-day vulnerability[7] is a security flaw that has not yet been patched, being unknown to the software developers or security researchers who would normally work to fix it. Users, being unaware of the vulnerability, have no way to protect themselves.

Zero-day exploits are digital attacks targeting zero-day vulnerabilities. Cybercriminals race to exploit these vulnerabilities to cash in on their schemes.

International initiatives maintain publicly available datasets about known vulnerabilities; the cybersecurity community has endorsed the Common Vulnerabilities and Exposures List (CVE)[8] which maintains a catalogue of publicly known cybersecurity vulnerabilities. The records in this catalogue are used to uniquely identify vulnerabilities, and publicise them in watchlists such as the Top 10 Web Application Security Issues by the Open Web Application Security Project (OWASP).[9]

Based on this analysis of vulnerability and exploits we can distinguish two different kinds of attack:

- Zero-click attacks[10] do not require any intervention by users. They are often based on a zero-day vulnerability, and are particularly dangerous, since users are usually unaware of such attacks, and thus cannot counter them or mitigate their effects.
- One-click attacks require an action by the users being targeted, which usually consist in clicking on a link or a button, presented through a web application. The victim, even though required to take an action, may not know what is happening, being fooled by the misleading appearance of the message or interface provided by the attacker.

In recent years, we have witnessed an increase in attacks, which have expanded beyond traditional channels (like email messages) to harder-to-avoid approaches (like automated "drive-by downloads" launched by infected webpages), enabling malicious actors to access, control, and infiltrate compromised devices, as well as collect large amounts of information from them.

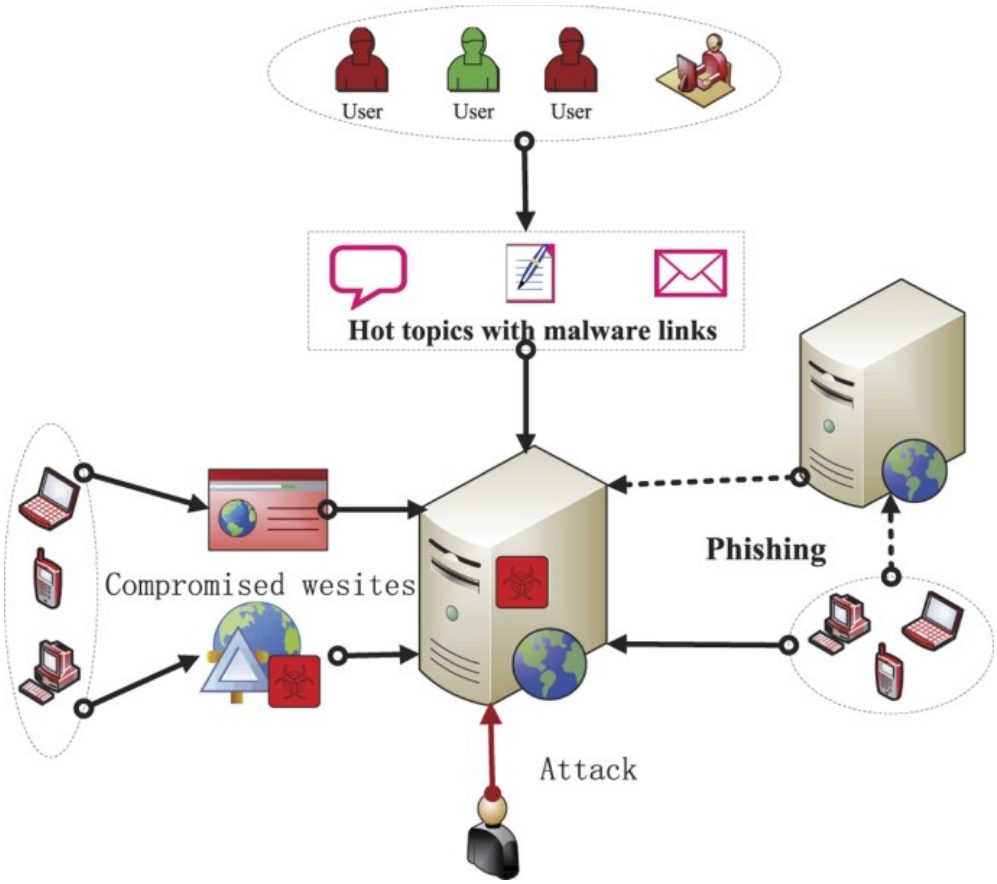
[7] Singh, U.K., Joshi, C. and Kanellopoulos, D. "A framework for zero-day vulnerabilities detection and prioritization. *Journal of Information Security and Applications* (2019), 46, pp.164-172.

[8] Common Vulnerabilities and Exposures List. https://cve.mitre.org/cve/.

[9] Open Web Application Security Project, https://owasp.org/www-project-top-ten/.

[10] Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. and Ng, A. "Cybersecurity data science: an overview from machine learning perspective." *Journal of Big data* (2020), 7(1), pp.1-29.

Figure 2: Diagram of web-malware spread mechanism[11]



2.3. New threats

Reports on cyber threats usually focus on the commercial domain, ignoring cyber threats to civil society,[12] even though spyware tools have been often aimed at dissidents, human rights defenders, journalists, and civil society advocates (see Section 3.2). Only recently, surveillance and attacks on civil society —through spyware incidents like Pegasus (see Section 3), Predator,[13] and others—have attracted media attention and prompted legislative/regulatory oversight.

In November 2022, the European Union Agency for Cybersecurity (ENISA) listed digital surveillance among the top ten emerging cyber security threats for 2030 (see Figure 3).[14] Similar worries are reported from many different sources.

[11] Liu, W. and Zhong, S. "Web malware spread modelling and optimal control strategies." *Scientific reports* (2017), 7(1), pp.1-19.

[12] ENISA. Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[13] Stevis-Gridneff, M. and Pronczuk, M. "Senior European Parliament Member Targeted as Spyware Abuse Spreads. "*The New York Times* (July 27, 2022). https://www.nytimes.com/2022/07/27/world/europe/eu-spyware-predator-pegasus.html.

[14] ENISA press release. *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!* November 11, 2022. https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030.

Figure 3: Cybersecurity Threats

Advanced Persistent Threat (APT) groups —i.e., the actors able to gain unauthorized access to computers and networks, remaining undetected for extended periods—, besides investing in developing or purchasing advanced offensive capabilities, increasingly adopt publicly available malicious tools, including open-source malware.[15] The widespread availability of low-cost, basic tools, has the effect that access to hacking and surveillance capabilities is expanded as barriers to entry are lowered. The wider access to the technology means that security researchers cannot timely identify these groups, which therefore can hide in the undergrowth.[16]

It is worth recalling that the NSO Group, the producer of Pegasus, is but one company in a much wider global cyber mercenary industry. In 2021, Meta shared information on seven actors that the company has removed from its platform as being suspected of surveillance.[17] Microsoft identified Candiru exploiting a zero-day vulnerability in 2021. Elaborate attacks are designed to inject spyware in targets' device. For instance, it has been claimed that in 2020 the website of the Iranian embassy in Abu Dhabi was modified by inserting in it a small software program having the function of injecting a spyware named Karkadann, similar to Candiru.[18]

---

15 Nimmo, B. "Meta's Adversarial Threat Report, Second Quarter 2022." Meta Newsroom. August 4, 2022. https://about.fb.com/news/2022/08/metas-adversarial-threat-report-q2-2022/.

16 Nimmo, B., Agranovich, D., Franklin, M., Dvilyanski, M. and Gleicher, N.. "Quarterly Adversarial Threat Report." *Meta*. August 2022. https://about.fb.com/wp-content/uploads/2022/08/Quarterly-Adversarial-Threat-Report-Q2-2022.pdf.

17 Agranovich, D. and Dvilyanski, M. "Taking Action Against the Surveillance-for-Hire Industry." *Meta Newsroom*. December 16, 2021. https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/.

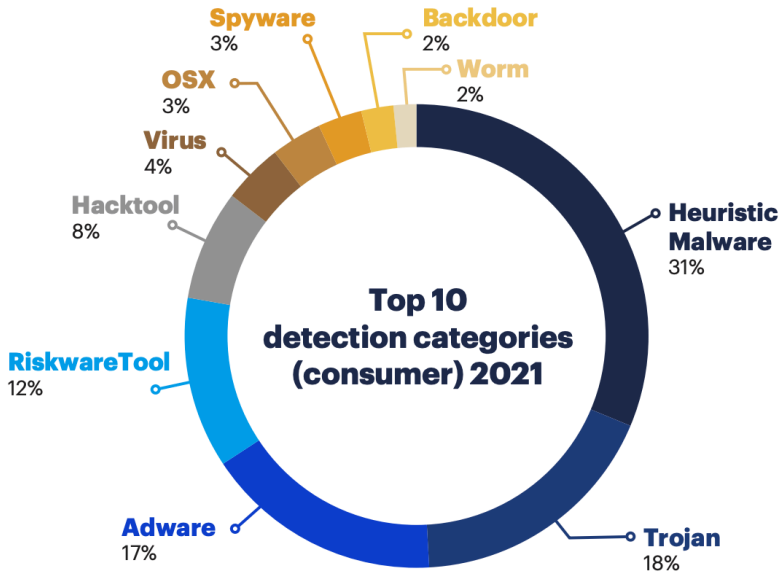
18 Faou, M. "Strategic Web Compromises in the Middle East with a Pinch of Candiru: ESET Researchers Have Discovered Strategic Web Compromise (aka Watering Hole) Attacks against High-Profile Websites in the Middle East." *welivesecurity*. November 16, 2021. https://www.welivesecurity.com/2021/11/16/strategic-web-compromises-middle-east-pinch-candiru/.

In 2021, Malwarebytes recorded the detection of 54,677 apps monitoring Android systems and of 1,106 apps spying over such systems (respectively, 4.2% and 7.2% more detections than in 2020). The 2021 appears to be the worst year on record for spyware. Some malware is pre-installed in the operating system run on mobile devices produced by budget manufacturers, which makes its removal very difficult.[19]

Three phases are common to manyy attacks: reconnaissance, engagement, and exploitation. While some entities specialize in one particular stage of surveillance, others support the entire attack chain.

1. Reconnaissance. The targeted individuals are profiled by hackers on behalf of clients, in order to identify the ways in which the devices of such individuals can be successfully attacked. In this stage, hackers usually deploy software to automate the data collection and analysis. They extract information from all available online records, such as blogs, social networks, knowledge management platforms, etc.
2. Engagement. The targeted individuals may be contacted with the purpose of instilling trust, acquiring information, and possibly tricking them into clicking on malicious links or files. To this end, attackers may resort to social engineering tactics. They may adopt fictitious personalities and connect with people via email, phone calls, text messages, or direct messages on social media.
3. Exploitation. The attackers deliver their malicious "payload," using their own custom-built exploits or using malicious tools purchased from others. Depending on the exploit, the attackers can access any data on the target's phone or computer, including passwords, cookies, access tokens, photos, videos, messages, address books, as well as silently activate the microphone, camera, and geo-location tracking.

Figure 4: Top ten detection categories in 2021 [20]

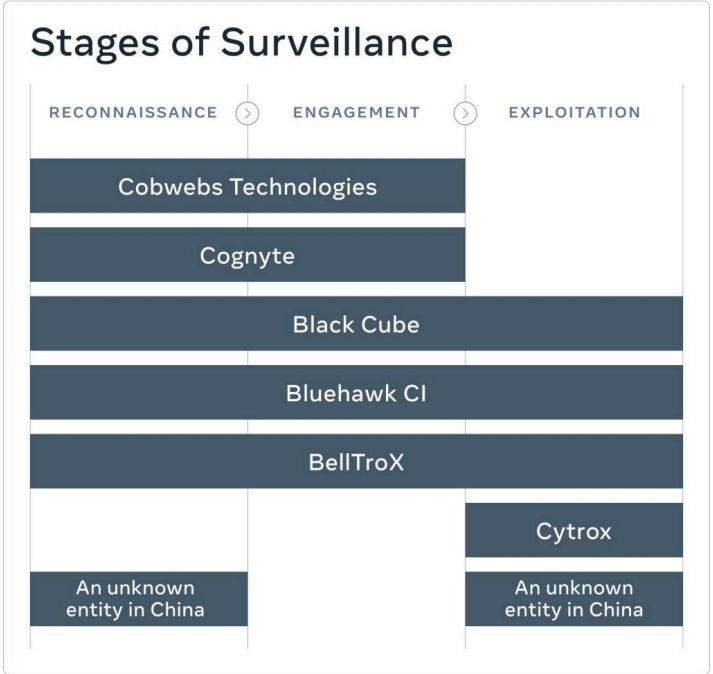


[19] Malwarebytes Cyberprotection. *Threat Review: Cyberprotection Starts with Understanding the Latest Attacks, Cybercrimes, and Privacy Breaches*. 2022. https://www.malwarebytes.com/resources/malwarebytes-threat-review-2022/index.html (retrieved December 26, 2022).

[20] Malwarebytes Cyberprotection. *Threat Review: Cyberprotection Starts with Understanding the Latest Attacks, Cybercrimes, and Privacy Breaches*.

Seven entities — located in China, Israel, India, and North Macedonia— were identified as monitoring individuals in over 100 countries exploiting the three stages in the surveillance chain, as shown in Figure 5.

Figure 5: Stages of surveillance and the seven entities identified by Meta[21]



[21] Nimmo, B. "Meta's Adversarial Threat Report"

3. PEGASUS AS A SURVEILLANCE TOOL

KEY FINDINGS

Targeted surveillance through technological tools raises justified concerns owing to its depth, as it can extend across all aspects of the life of the targeted individuals. Spyware systems hacking mobile devices —such as Pegasus, developed by the Israeli NSO Group— enable a pervasive secret surveillance. Pegasus has full and unrestricted access to the targeted device: it can extract all data in it (initial data extraction), monitor all activities performed through it (passive monitoring), activate the device's functionalities to collect further data (active monitoring), and possibly interfere with the content of the device and the messages it sends. It can be installed without any action by the individuals concerned and leaves no (or few) traces of its operation. Extensive evidence exists of the use of Pegasus in many countries, including EU Member States.

In this section, we will first introduce the notion of surveillance. We distinguish, on the one hand, traditional and new, technology-enabled surveillance, and on the other hand, targeted and mass surveillance. Then we will focus on Pegasus as an extreme instance of technology-enabled targeted surveillance.

3.1. Traditional and new surveillance

To counter national security risks—but also to engage in activities aimed at obtaining political or economic advantages—governments have always relied on covert investigation methods. Such methods are often deployed for the purpose of "surveillance,"[22] i.e., for the deliberate, systematic, and sustained scrutiny of individuals and groups, involving "attention to personal details for purposes of influence, management, protection or direction."[23]

The deployment of human agents to collect information through infiltration, personal contact, and access to confidential documents has been supplemented with technology, and in particular with digital technologies. Thus, traditional surveillance, based on unaided human senses, has given way to a very different social-control model called "new surveillance," which has been defined as the "scrutiny of individuals, groups, and contexts through the use of technical means to extract or create information," thus overcoming spatial, temporal, quantitative, and other limitations of traditional surveillance.[24]

Todays' information technologies enable to an unprecedented degree the exercise of "communications surveillance," which the UN High Commissioner for Human Rights describes as follows:

---

[22] The word *surveillance*—from the French *surveiller*, composed of *sur*, meaning "over," and *veiller*, from the Latin *vigilare*, meaning to watch over—came into the English language during the French Revolution (1789–99), when surveillance committees were established in every French municipality to monitor the actions and movements of foreigners, dissidents, and suspected persons. See: Watt, E. *State Sponsored Cyber Surveillance*. Elgar, 2021. On cybersurveillance and national security, see also Monti, A. and Wacks, R. *National Security in the New World Order*. Routledge, 2022.

[23] Lyon, D. *Surveillance Studies.* Polity Press, 2007.

[24] Marx, G. T. *Windows into the Soul. Surveillance and Society in an Age of High Technology*. Chicago University Press, 2016.

> *the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present or future.*[25]

It is true that massive surveillance has been possible before the advent of present technologies, as in the case of the German Democratic Republic's Ministry for State Security, known as the Stasi, which amassed archives containing files on an estimated 6 million people.

> *Among an estimated 274,000 employees were at least 174,000 informants, which would have been about 2.5% of the working population. Informants snooped in every office, cultural and sporting society, and apartment building. They recorded people in their own homes and in the homes of their friends.*[26]

Modern surveillance, relying on digital technology, can achieve and surpass this level of pervasiveness with a fraction of the manpower. Sensors and hacking software can collect any kind of information directly from the spied-on individual, with limited or no human intervention, while massive quantities of electronic communications can be obtained directly from the cables that deliver such communications and the servers that store them.

A key distinction in the analysis of surveillance is that between targeted and mass surveillance.

Targeted surveillance is directed at specific persons of interest. It can consist in intercepting communications originating from a particular person or location, but it may as well include remote equipment interference (also known as "hacking"), which is used to extract data from Internet-connected devices such as desktops, laptops, tablets, or smartphones. As digital communications are increasingly encrypted, security and law-enforcement agencies tend to rely on equipment interference to access the content of communications before it is made inaccessible through encryption. Advanced spyware such as Pegasus represent the current evolution of technologies that have been in use for a few decades.

Unlike targeted surveillance, mass surveillance is indiscriminately aimed at large groups of people (and may even include an entire nation). It starts without any suspicion about a particular person or persons and has a proactive function, being aimed at identifying future threats and flagging individuals as suspect. Mass surveillance has been enabled by digital technologies which can process huge amounts of data in a short time and with a limited cost, collecting such data from telecommunication lines or from existing information repositories (often held by leading digital companies). Mass surveillance has been the object of a vast global contestation, especially after the Snowden revelations exposed the breath of the phenomenon and the extent of abuses. The EU Parliament expressed its concerns about surveillance with regard to its impact on fundamental rights and principles of EU law.[27] Both the

---

[25] United Nations. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/23/40, 2013.

[26] Amnesty International. *Lessons from the Stasi—a cautionary tale on mass surveillance*. 2015, url: https://www.amnesty.org/en/latest/news/2015/03/lessons-from-the-stasi/

[27] See European Parliament (2014). *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)); EU Agency for Fundamental Rights. Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU. Volume II: Field perspectives and legal update*. Publications Office of the European Union, 2017.

European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (ECJ) have in several cases issued opinions against overbroad surveillance by states.[28]

By contrast, targeted surveillance, which is the focus of this report, was not in the spotlight until recently. However, recent technological developments—as evidenced by software such as Pegasus—require us to also consider the individual and social impacts of targeted surveillance. In fact, if mass surveillance raises legitimate concerns owing to its *breadth*, as it can extend across all members of a community, targeted surveillance, with the technological tools available to it, raises equally legitimate concerns owing to its *depth*, as it can extend across all aspects of the life of the targeted individuals.

3.2. The challenge posed by spyware

Spyware systems that hack mobile devices, as in the case of Pegasus, enable a pervasive surveillance. Their impact on the individuals concerned and on society as a whole is potentially enormous, threatening to undermine the EU's fundamental rights as well as the core values of EU law.

The depth of their impact can only be understood by considering that human life today unfolds in a hyperconnected world, in which many, if not most, individual and social activities are mediated by the digital infrastructure, which we use to store and share a vast array of information, as well as to communicate and interact both orally and in writing. Here a special role is played by our personal devices, typically smartphones, since they are the interface through which we access the digitally mediated and constituted dimension we inhabit.

It may seem that device-hacking technologies can be assimilated to traditional wiretapping, a technique to secretly access communications that has been largely used by law enforcement agencies and national security services since the development of telecommunication networks. Wiretapping, broadly understood, consists in secretly accessing the content of a message transmitted over communication lines and sending a copy of it to the intercepting agency. Originally, wiretapping involved setting an electrical device (the tap) on the telephone line, but today the operation can be performed remotely, thanks to digital switching technologies, which are activated by communications operators. This practice is regulated by national laws and contemplated in supranational instruments, such as the Council Resolution on Lawful Interception.[29]

However, important differences exist between wiretapping and device hacking, since the latter makes it possible to collect a larger body of information: apart from accessing messages on the attacked device, hacking can also access and possibly manipulate *all* the information stored on it. Device hacking is carried out to collect a larger set of data, but also to overcome encryption technologies, as noted in Section 3.1. In end-to-end-encryption, the original communication, before being sent, is transformed into a ciphertext, which is not understandable to third parties: to recover the original communication, the ciphertext must be decrypted using a secret key which is only available to the receiver. Device hacking makes it possible to circumvent encryption by capturing the original messages *before* they are encrypted. In contexts in which criminal activities rely on advanced encryption technologies, a justification may exist for device hacking to be used to counter the most serious crimes and national

[28] Among the most recent cases for the ECtHR, see *Big Brother Watch and Others v. The United Kingdom* [GC] (nos. 58170/13, 62322/14 and 24960/15, 25 May 2021); for the Court of Justice, see *Commissioner of the Garda Síochána and Others* (C-140/20, 5 April 2022).

[29] Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01).

security threats. However, as we will see in the following, in the absence of strict limitations and effective controls, the practice of device hacking is hardly compatible with the EU legal framework, and more generally with the preservation of democracy and human rights.

3.3. Critical features of Pegasus

According to the European Data Protection Supervisor (EDPS) we can distinguish three notable features of Pegasus that give it "the potential to cause unprecedented risks and damages not only to the fundamental freedoms of the individuals but also to democracy and the rule of law,"[30] namely, its ability to (a) gain *complete* access to the devices it targets, (b) carry out zero-click attacks, and (c) leave little or no trace behind. Let us look at each of these in turn.

3.3.1. Complete access

The first feature is that Pegasus has "complete, unrestricted access to the targeted device,"[31] as has emerged from investigations carried out by Amnesty International's Security Lab.[32] According to the product description made available by the Security Lab,[33] there are three ways in which Pegasus can collect data:

- *Initial data extraction*, which collects all the information already available on the device at the time of Pegasus's installation, including SMS records, contacts details, call history (the call log), calendar records, emails, instant messaging, and browsing history.
- *Passive monitoring*, which collects in real time any new records that become available while the spyware remains in function (this includes the same information as above, plus location tracking based on cell-id, i.e., the number identifying the nearby transceiver station to which the phone connects to access a communications network).
- *Active monitoring*, which consists in using the functionalities of the targeted device to perform further data-collection activities, such as tracking location using GPS, recording voice calls, retrieving files, recording environmental sounds, taking photos, and capturing screens.

[30] EDPS. Preliminary remarks on modern spyware, 2022. https://edps.europa.eu/system/files/2022-02/22-02-15edpspreliminaryremarksonmodernspywareen0.pdf

[31] EDPS. Preliminary Remarks, p. 3.

[32] Amnesty International. *Forensic Methodology Report. How to Catch NSO Group's Pegasus*. Amnesty International, 2021. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[33] Pegasus – *Product Description*.

Figure 6: Data collection through Pegasus[34]

As shown in Figure 6, Pegasus provides for a level of surveillance and manipulation that was previously unthinkable. Hannah Arendt famously wrote that "[e]verything that lives needs the security of darkness to grow at all."[35] Indeed, Pegasus leaves nothing in darkness.

3.3.2. Zero-click attacks

Pegasus enables so-called zero-click attacks, meaning that it can be installed without any action by the individuals concerned: no need for them to click on an alert or answer a message (see Figure 7). Here is how this feature is described in the Pegasus description:

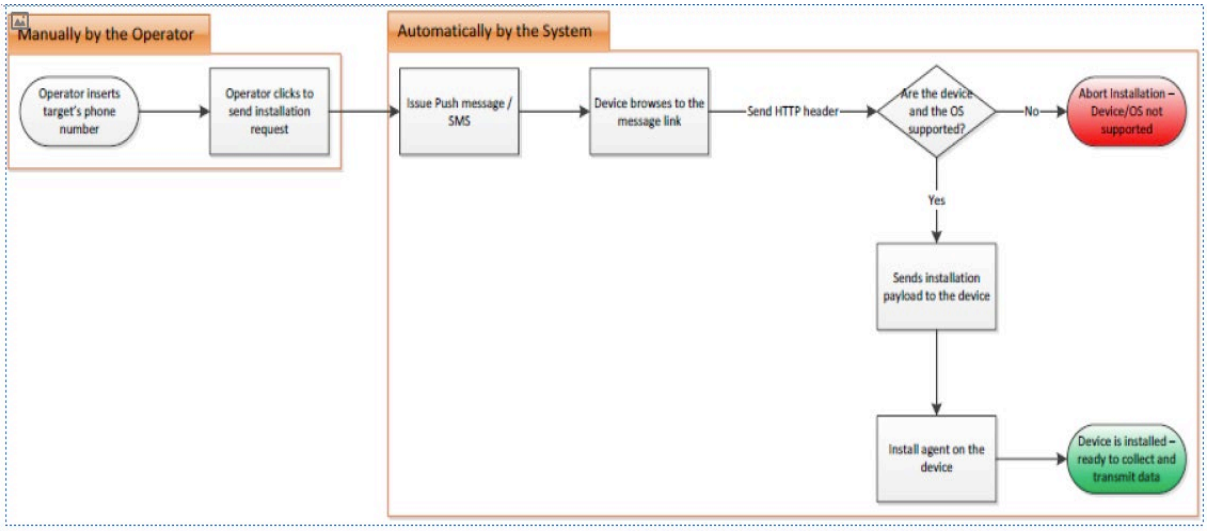
> *A push message is remotely and covertly sent to the mobile device. This message triggers the device to download and install the agent on the device. During the entire installation process no cooperation or engagement of the target is required (e.g., clicking a link, opening a message) and no indication appears on the device. The installation is totally silent and invisible and cannot be prevented by the target.*[36]

[34] Pegasus – *Product Description*, p. 16.

[35] Arendt, H. "The Crisis in Education." *In Between Past and Future: Six Exercises in Political Thought. Viking*, 1961 [1954].

[36] Pegasus – *Product Description*, 12.

Figure 7: Installation of the Pegasus agent[37]



Thus, even a careful and digitally savvy user may have no clue that their device is being controlled by the spyware. Through the work of Amnesty International and Toronto's Citizen Lab,[38] among others, it has been possible to identify different zero-click exploits, i.e., pieces of software and data that gain control of user devices, exploiting their vulnerabilities, without users doing anything specific. These exploits download the Pegasus agent (the piece of Pegasus software installed on the victim's device), which collects the data and interacts with the remote Pegasus servers (see Figure 7 and Figure 8). Even the biggest and technologically most advanced ICT companies—such as Google and Apple—have so far been unable to provide effective preventive protections, since the leading spyware companies can rely of high-level skills, on a par with those of a country's intelligence agencies.[39]

3.3.3. No (or few) traces

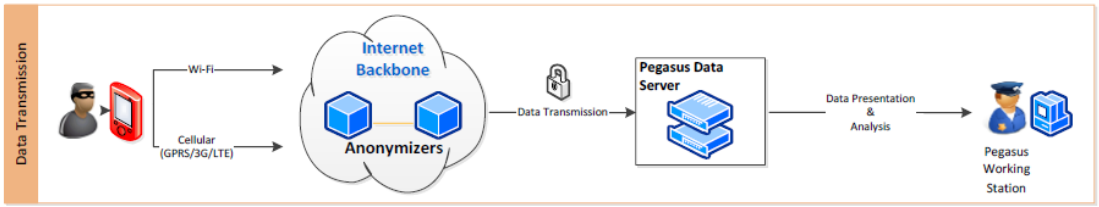
It is very difficult to detect a Pegasus installation, obtain evidence of its activities, and identify the authors of the intrusion, unless the attacked system has a secure logging function (a function that records all of a device's activities), as seems to have been the case for Apple phones. In fact, during uninstallation, Pegasus tries to remove all traces of its presence. According to the EDPS, new versions of Pegasus may be even more difficult to detect, being only temporarily installed, or residing in the cloud. Finally, identification of Pegasus's remote operators is made impossible by the use of a network anonymising the link between the Pegasus agent and the Pegasus server (Figure 8).

[37] Pegasus – *Product Description*, 13.

[38] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto.

[39] Newman, L. H. "Google Warns That NSO Hacking Is On Par With Elite Nation-State Spies." In *Wired* (15 December 2021).

Figure 8: The Pegasus data-collection process[40]



3.3.4. A multi-layered open environment

The infrastructure used by Pegasus (and by other similar device-hacking technologies) is relevantly different from the technological frameworks for traditional wiretapping. When intercepting communications passing through telephone lines, competent officers can usually rely on certified and controlled equipment, and on the transparent cooperation of telecommunication operators. This is often not the case where law enforcement or national security services use "special investigation techniques," and in particular when they hack computer devices to collect data and monitor communications. A system such Pegasus operates through a multitude of networks and privately owned hardware (including the hardware of the victim), without an agreed-upon framework involving telecommunication companies. Thus, it may be argued that Pegasus does not ensure the security of communications and thus does not guarantee that the collected data will not be unlawfully modified or used for additional purposes.

3.3.5. Content manipulation

As noted, Pegasus can take control of the targeted device and make use of its functionalities. This enables it to engage in active monitoring, e.g., it can instruct the device microphone and camera to record information from the environment.

Moreover, Pegasus's control over a device could in principle be used to implement multiple unlawful purposes: to modify the device's content, creating and storing fake messages or other documents; to send fake messages, impersonating the device owner; to gain access to the owner' digital or physical assets and possibly execute transactions in the owner's name; or to plant false evidence of crimes or other unlawful activities on the device.[41]

3.3.6. The use of Pegasus

As mentioned, Pegasus is developed by the Israeli company NSO,[42] who sells it to governments all over the world, such sales being authorised by the Israeli Ministry of Defence. NSO claims that under its contractual clauses, Pegasus may only be used to fight terrorism and crime (though, as we will see, extensive evidence exists of Pegasus being used for other purposes). It has stated that it has sold Pegasus to 60 government agencies in 40 countries.

---

40 Pegasus – *Product Description*, 13.

41 EDPS. *Preliminary Remarks on Modern Spyware*, p. 3.

42 NSO stands for Niv, Shalev and Omri, the company's founders.

The extent of Pegasus's use (and abuse) first emerged through a 2018 inquiry by Citizen Lab of the University of Toronto, which found clues pointing to Pegasus in 45 countries, some of which under authoritarian regimes.

According to a 2021 report issued by the Pegasus Project —a collaborative initiative undertaken by more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories, with the technical support of Amnesty International— Pegasus spyware has been widely used by governments all over the world to target human rights activists, opposition figures, lawyers, judges, and foreign leaders.[43] The Pegasus Project also published a list of that 50,000 phone numbers that appear to belong to individuals who had been selected by clients of the Israeli NSO Group as possible targets of surveillance.

The European Parliament established the PEGA Committee of inquiry, tasked to investigate the use of Pegasus and equivalent surveillance spyware.[44] According to an inquiry by the Committee, there is strong evidence of the use of Pegasus in the EU. It appears that the NSO Group has sold its products to 22 end-users in at least 14 Member States, among which are Poland, Hungary, Spain, the Netherlands, and Belgium. Two Member States, Cyprus and Bulgaria, have served as export hubs for the spyware.[45]

Some actions against the abuses committed through Pegasus have been started in the US, where in 2021 the NSO Group was blacklisted for engaging in activities that are contrary to the national security or foreign policy interests of the United States (it was thus excluded from contracts with US agencies and business with US companies). This is a significant change in US policy, since it appears that the US itself had entered negotiations to buy Pegasus and had even acquired it for the government of Djibouti. However, it seems that US agencies continue to use spyware having similar functions, such as Graphite, developed by the Israeli company Paragon.[46] Also in 2021, both Apple and Meta filed lawsuits against the NSO Group for surveillance and targeting of their users. In June 2022, a United States district court rejected the NSO Group's claim to immunity in the Apple lawsuit.

In November 2021, it emerged that Israel removed 65 countries from its list of countries to whom cyber products can be exported, reducing the number from 102 to 37. Still, it has been reported in the media that Israel re-authorised Saudi Arabia to use Pegasus.

[43] Amnesty International. Forensic Methodology Report. *How to Catch NSO Group's Pegasus*. 2021

[44] PEGA (Committee of Inquiry to Investigate the use of Pegasus and Equivalent Surveillance Spyware). https://www.europarl.europa.eu/committees/en/pega/home/highlights.

[45] European Parliament. Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware Rapporteur: Sophie in 't Veld (2022). *Draft Report*.

[46] Mazetti, M., Bergman, R., and Sevis-Grindneff, M. "US strains to control spyware, but uses it." *The New York Time* (1 December 2022). s.

4. PEGASUS AND (DELIBERATIVE) DEMOCRACY

KEY FINDINGS

Pervasive surveillance affects not only people's privacy and data protection rights, but also further individual rights —such as the rights to freedom of speech, association, and assembly— as well as the democratic makeup of society (which presupposes the exercise of such rights).

Political participation is affected by spyware in that spied-on citizens can be intimidated into abstaining from engaging in interactions having political content, from sincerely expressing their views, and from associating with others for political purposes. This affects the quality of a democratic public sphere, which ultimately relies on the citizens' inputs and reactions.

More specifically, spyware is often used to attack individuals (like journalists, politicians, and activists) who play a special role in the public sphere. Surveillance of such individuals opens space for repression, manipulation, blackmailing, falsification, and defamation.

The electoral process itself may be affected where the collected information, which may be manipulated, is used to carry out smear campaigns against unwanted candidates or other actions negatively affecting their chances of success. The mere fear of being spied on may induce people to refrain from running for office or from running an effective campaign.

Pervasive surveillance affects not only people's privacy and data protection rights, but also further individual rights —such as the right to freedom of speech, association, and assembly—as well as the democratic fabric of society (which presupposes the exercise of such rights).

The connection between data protection and democracy has always been a key aspect of the data protection debate,[47] while growing increasingly important in recent years, as society has become more and more digital, and surveillance technologies more and more powerful:

> *Neither freedom of speech nor freedom of association nor freedom of assembly can be fully exercised as long as it remains uncertain whether, under what circumstances, and for what purposes, personal information is collected and processed. Considerations of privacy protection involve more than any one particular right: they determine the choice between a democratic and an authoritarian society.*[48]

In the aftermath of the Snowden revelations, the Parliamentary Assembly of the Council of Europe, in its Resolution 2045, stated that the surveillance practices engaged in by states endanger human rights, which are the "cornerstones of democracy" and whose "infringement without adequate judicial control also jeopardises the rule of law."[49]

In the following sections we will be considering how surveillance —particularly through Pegasus— may seriously affect the ecology of a democracy, interfering with different aspects of it.

---

[47] See: Simitis, S. "Reviewing Privacy in the Information Age." In *University of Pennsylvania Law Review* (1987), pp. 707-46; Rodotà, S. "Data Protection as a Fundamental Right." In *Reinventing Data Protection*? Ed. by Serge Gutwirth et al. Springer, 2009, pp. 77–82.

[48] Simitis. "Reviewing Privacy in the Information Age," p. 734.

[49] See: Council of Europe. *Mass surveillance: Who is watching the watchers?* Council of Europe Publishing, 2016.

4.1. The idea of participatory-deliberative democracy

To understand the way in which surveillance may affect democratic processes, it may be useful to refer to the kind of social arrangement that is required for democracy to be effective. While many definitions of democracy and many approaches to it exist,[50] here I will focus on the idea of deliberative democracy, which offers a broad normative framework for approaching political participation, and so also for understanding its failures. The concepts of deliberation and deliberative democracy can be defined as follows:

> *We define deliberation minimally to mean mutual communication that involves weighing and reflecting on preferences, values, and interests regarding matters of common concern. Deliberative democracy incorporates the requirements that deliberation take place in contexts of equal recognition, respect, reciprocity, and sufficiently equal power for communicative influence to function.*[51]

Thus, on the ideal of deliberative democracy, public choices should be supported by appropriate public justifications, so that "the forceless force of the better argument"[52] may ultimately prevail, or at least there is a propensity to listen to arguments and move towards reasonable outcomes. Political decisions should indeed be the outcome of open and inclusive processes, in which different opinions are raised and discussed, on the basis of reasons that citizen can understand, so that "persuasion that raises relevant considerations should replace suppression, oppression and thoughtless neglect."[53] The promotion of participatory and deliberative democracy is indeed one of the goals of the Commission's 2020 European Democracy Action Plan.[54]

From the perspective of a liberal and deliberative approach, the institutional design of modern democracies should guarantee three fundamental aspects:

> *first, the private autonomy of citizens, each of whom pursues a life of his or her own; second, democratic citizenship, that is, the inclusion of free and equal citizens in the political community; and third, the independence of a public sphere that operates as an intermediary system between state and society.*[55]

---

[50] Among recent reviews see, for instance: Beckman, L. "Democracy." In *Oxford Research Encyclopedias, Politics*. Oxford University Press, 2021; Christiano, T. and Sameer B. "Democracy." In *The Stanford Encyclopedia of Philosophy*, Stanford University, 2022.

[51] Bächtiger, A. et al. "Deliberative Democracy: An Introduction." In *The Oxford Handbook of Deliberative Democracy*. Oxford University Press, Sept. 2018, p. 1.

[52] Habermas, J. *Legitimation Crisis*. Cambridge, Beacon Press, 1975, p. 108.

[53] Mansbridge, J. et al. "A systemic approach to deliberative democracy." In: *Deliberative Systems: Deliberative Democracy at the Large Scale*. Ed. by J. Parkinson and J. Mansbridge. Cambridge University Press, 2012.

[54] Commission of the European Communities. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*. COM(2020) 790 final, 2020.

[55] Habermas, J. *Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research. In: Communication Theory* (2006), p. 412.

4.2. The impact of pervasive surveillance on democracy

It is easy to see that that participatory-deliberative democracy stands to be seriously affected by pervasive surveillance through spyware like Pegasus.

Let us first consider the situation of all individuals who may have a reasonable suspicion that they are under surveillance, i.e., that their devices have been hacked or may be hacked in the near future, in such a way that all of their life may be observed with malicious intent. This will engender in such individuals a fear of being subject to adverse actions, should unwanted behaviour be detected, or should circumstances be detected that provide new opportunities to harm them (as by attacking their reputation or anticipating their actions). Such adverse actions may include legal or social sanctions, the imposition of losses (dismissals, foreclosed opportunities), defamation, and unlawful and possibly violent attacks. Under such conditions, people may refrain from any activity that might possibly be detected and attract harmful reactions. In this regard, people sometimes speak of a Panopticon effect (with reference to the prison designed at the end of the 18th century by philosopher Jeremy Bentham, where prisoners were visible to the guards but could not see whether at any given moment they were actually being watched): the mere possibility of being kept under watch and "punished" puts pressure on individuals to behave according to what they believe is expected of them.

Moreover, cases in which surveillance has adversely affected certain individuals provide lessons for all those who believe that they, too, might be subject to similar measures. All potential victims of surveillance learn that they should not engage in behaviour that may lead them to be subject to surveillance. Moreover, they learn that they should not engage in behaviour which, if observed by surveillance, may lead to adverse social, political, or legal effects. Being subject to these risks may induce people to avoid engaging in social and political issues, to self-censor and avoid expressing opinions even in private contexts, and to choose to "hide while living," remaining outside the public sphere.

By so affecting individuals, spyware also affects the democratic-deliberative makeup of society, in a way that depends on the specific role that different individuals play within such a makeup. Indeed, recent work on democratic theory adopts a systemic approach to deliberative democracy: a healthy deliberative democracy requires multiple segments of society to contribute in different ways, to ensure that societal choices are based on considerate publicly available reasons, produced through an inclusive process. Pervasive surveillance, and in particular the use of Pegasus-like spyware, can strongly affect the working of different aspects of a democratic arrangement.

For one thing, spyware can affect the first of the three previously identified aspects, namely, the *private autonomy* of individuals, i.e., their private choices and interactions. By interfering with the private autonomy of individuals, spyware has an impact on democracy insofar as democracy is premised on the idea that people are able to autonomously make their life choices (relating to family, work, leisure, etc.) and interact informally with others, and can accordingly develop their interests and ideas. Only if they can develop their personality, free from undue external pressure, can they then make genuine contributions to the public sphere.

But being under pervasive surveillance also affects the second of the three aspects, namely, *democratic citizenship*. We need to consider in this regard that democratic citizenship involves "the political participation of as many interested citizens as possible through equal communication and participation rights; periodic elections (and referendums) on the basis of an inclusive suffrage; the

competition between different parties, platforms, and programs; and the majority principle for political decisions in representative bodies."[56]

Political participation is affected by spyware in that spied-on citizens can abstain from engaging in interactions having political content, from sincerely expressing their views, and from associating with others for political purposes. This would prevent citizens from exercising their freedoms of expression and association. Additionally, it will affect the quality of a democratic public sphere, which ultimately relies on the citizens' input and reactions.

By interfering with the communication that citizens, media outlets, and politicians engage in, and subjecting them to undue influence for political purposes, spyware also undermines the third of the three aspects, namely, the *independence of the public sphere*.

To understand how all of this may happen, we need to consider that, as noted, a deliberative-democratic arrangement is an ecology resulting from a combination of different components: only when each of them adequately performs its function will a healthy democratic environment result.

> *The center of the political system consists of the familiar institutions: parliaments, courts, administrative agencies, and government. Each branch can be described as a specialized deliberative arena* [...]. *At the periphery of the political system, the public sphere is rooted in networks for wild flows of messages —news, reports, commentaries, talks, scenes and images, and shows and movies with an informative, polemical, educational, or entertaining content. These published opinions originate from various types of actors— politicians and political parties, lobbyists and pressure groups, or actors of civil society. They are selected and shaped by mass-media professionals and received by broad and overlapping audiences, camps, subcultures, and so on.*

In this context

> *pro or con attitudes to controversial public issues as they tacitly take shape are influenced by everyday talk in the informal settings or episodic publics of civil society at least as much as they are by paying attention to print or electronic media.*

While every citizen can play a role in the public sphere, politicians and media professionals tend to occupy the centre of the political system, as both co-authors and addressees of public opinion. To a large extent, this continues to be so even today, where the Internet provides everybody with the ability to post information and comments through forums, blogs, online repositories, social networks, etc.

Finally, elections serve a necessary function within every democratic-deliberative arrangement: they ensure that public opinion remains relevant to public decision-making by enabling voters to select representatives whose views align with their own.

The case of Pegasus, and of other similar spyware, shows how all these different processes of a democratic ecology can be —and indeed have been— interfered with.

First, the possibility of being spied on affects in a broad sense the political activity of all individual citizens. Because of surveillance, they may refrain from accessing and distributing political information (considering that Internet browsing and digital communications could be monitored) and may steer clear of political interactions, from everyday talk in informal settings to participation in political movements and collective action.

[56] Habermas J. *Political Communication in Media Society*, p. 412.

More specifically, spyware affects those individuals who, as noted, play a special role in the public sphere. In fact, it has often been used against journalist and politicians, and more generally people involved in political activism. Surveillance of such individuals opens space for repression, manipulation, blackmailing, falsification, and defamation. This negatively affects not only the individuals concerned but also the process of opinion formation in the public sphere. Spied-on journalists may be unable to do their reporting —for fear that their confidential contacts are tracked, for example, or because of obstacles they meet in their investigative work— or they may refrain from publishing stories for fear of adverse reactions based on confidential information collected from their devices. Similar considerations apply to politicians, when viewed in their role as contributors to the public communication sphere. When spyware is deployed by the dominant political forces against their adversaries, a foundational —though always imperilled— aspect of a democratic arrangement is also imperilled, namely, the separation between the media and political power.

Spyware may directly impinge on the functioning of the core institutions in a democratic arrangement, namely, legislatures and the judiciary. Attacks may be directed against people already serving as elected representatives or judges: some may experience adverse actions based on the collected information; others may just fear being spied on. In either case, the individuals concerned may refrain from acting in keeping with the standards of their role as legislators or judges, which standards, in the first case, required them to regulate society for the common good of its citizens, while respecting constitutional constraints, and in the second case require them to impartially adjudicate disputes according to the law.

Finally, the electoral process itself may be affected where the collected information, possibly manipulated, is used to carry out smear campaigns against unwanted candidates or to engage other actions diminishing their chances of success in the elections (to the benefit of their adversaries).[57] Moreover, the mere fear of being spied on may induce people to refrain from running for office or from running an effective campaign. This may impinge on the fairness and equality of the electoral process, since individuals and parties who can avail themselves of spyware —directly or thanks to their connections with those in government— will have an advantage over competing individuals and parties who are spied on. Spyware can enable various modes of "cyber election meddling."[58] In particular, by extracting private information from the victims' devices, spyware makes it possible to take the first step in "doxing,"[59] namely,

> *the practice of gaining unauthorized access to a computer system or digital service such as a social media or email account, exfiltrating non-public data, and subsequently leaking the data to the public*.

In fact, from investigations into Pegasus, it has emerged that materials obtained though the spyware have enabled two kinds of malicious doxing (as opposed to whistleblowing in the public interest): "strategic hacks," which consist in selectively leaking materials that are of interest to the public, but for the purpose of advancing partisan political interests, and "tainted leaks," which consist in deliberately including false or otherwise misleading information within a larger set of genuine confidential data

[57] A very famous example of an interference through unlawful tapping in an electoral process is provided by the Watergate case (1972). The intrusion in the headquarters of the Democratic National Committee and the installation of wiretapping devices led to the resignation of the US president Richard Nixon.

[58] For a discussion and classification of various kind of "cyber election meddling," along with references, see: Sanders, B. "Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections." In *Chinese Journal of International Law* (2019); Watt, Eliza. *State Sponsored Cyber Surveillance*, Section 2.4.3.

[59] The term *doxing* or *doxxing* derives from the slang *dropping dox*—where *dox* stands for "docs" (documents)—i.e., the unsolicited distribution of confidential information (documents).

that is leaked to the public. In the latter case, the doxing can also be viewed as an instance of misinformation, which is the practice of spreading

> *verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public and may cause public harm [… including] threats to democratic, political and policy making processes.*[60]

Misinformation seems to play an increasing role in electoral processes, where it is used to discredit politicians and parties in the opposite camp, and more generally to spread false or misleading information favouring one side, to the detriment of its opponents:

> *Disinformation now forms part of a wider array of tools used to manipulate electoral processes, such as hacking or defacing websites or gaining access to and leaking personal information about politicians. Cyber-enabled operations may be used to compromise the integrity of public information and prevent the identification of disinformation sources. This is critical during election campaigns, where compressed schedules may prevent timely detection of disinformation and response.* [61]

4.3. Some evidence of interference in democratic processes through Pegasus

Investigations by the *Guardian* and other 16 media organisations suggest widespread and continuing abuse of Pegasus to influence party politics and the media. A list has been leaked containing more than 50,000 phone numbers that appear to belong to individuals who had been selected by clients of the Israeli NSO Group as possible targets of surveillance.

This list has been found to include not only terrorists and known criminals but also hundreds of business executives, religious figures, academics, NGO employees, and union and government officials, including cabinet ministers, presidents, and prime ministers. Among them are more than a hundred journalists, including reporters, editors, and executives of leading journals.

According to a report to the European Parliament,[62] Greece has been accused of targeting journalists, as well as politicians in the opposition through the device-hacking spyware.[63] Politicians from Hungary, France, Spain, Finland, Poland, Belgium, and the European Commission have allegedly been victims of Pegasus attacks.

In particular, the report cites investigations according to which more than 300 persons have been targeted by Pegasus in Hungary, among whom journalists, politicians, academics, lawyers, and government officials.

---

60 European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling online disinformation: a European approach*. COM(2018) 236 final, 2018.

61 European Commission. *Communication on Tackling online disinformation*, Section 3.2.

62 Marzocchi, O. and Mazzini, M. *Pegasus and surveillance spyware.*

63 In Greece the evidence points to Predator. A piece of spyware similar to Pegasus, Predator too is developed by Israeli software companies (operating under the name Intellexa). See Benjakob, O. "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer Is Building a New Empire", *Haaretz* (September 2022), available at: https://www.haaretz.com/israel-news/security-aviation/2022-09-20/ty-article-magazine/.highlight/as-israel-reins-in-its-cyberarms-industry-an-ex-intel-officer-is-building-a-new-empire/00000183-5a07-dd63-adb3-da173af40000

Similarly, the report observes that according to Citizen Lab, the Polish government has used Pegasus to put many Polish citizens under surveillance, including lawyers, prosecutors, members of Parliament, and leaders of political parties.

Among the testimonies given to the Polish Senate's Special Committee was that of Prof. Zoll, who argued that Pegasus is illegal in Poland due to its lack of certification and to the potential it affords for leakages and manipulation of data. Moreover, he testified that the use of Pegasus interfered with the 2019 elections, significantly altering the equal position of candidates in the electoral process and the fairness of its outcome. The candidates who were targeted through Pegasus were in fact at disadvantage relative to their opponents, especially where the latter, due to their political connections, could avail themselves of the collected data to anticipate and discredit the former candidates.

Senator Krzysztof Brejza gave testimony at a PEGA meeting of 27 Oct. 2022 titled "The Impact of Spyware on Fundamental Rights / Democracy and Electoral Processes." He stated that he had been subjected to pervasive surveillance during the 2019 elections, including wiretapping, theft of correspondence, and falsification of it. The data obtained through surveillance, and in particular text messages obtained through Pegasus, were selectively and misleadingly presented in the context of a defamatory campaign meant to influence elections. His testimony exemplifies the depth of the impact of surveillance on the activity of individual actors, and consequently on the functioning of democratic institutions.

5. NATIONAL SECURITY: JUSTIFICATION OR PRETENCE?

KEY FINDINGS

The use of spyware is usually justified by invoking national security. However, it appears that in many cases spyware is used for other purposes, and in particular for objectives pertaining to partisan political interests or to the repression of social and political dissent.

To prevent an excessively expansive use of the notion of *national* security, this notion should be understood restrictively and distinguished from the concept of *internal* security, the latter having a broader scope, including the prevention of risks to individual citizens, and in particular the enforcement of criminal law.

It has been recognised that many states have used national security as a legal pretext to curtail freedom of expression, legitimise torture and other ill-treatment, and exert a chilling effect on minorities, activists, and political opposition.

In particular, extensive evidence exists on Pegasus being used to target individuals —such as political opponents, human rights activists, lawyers, and journalists— who have no connection to serious crimes and pose no national security threat.

In this section, first we discuss the concept of national security and then we consider its use as a justification for state action, including cases in which, under the banner of alleged national security interests, different purposes are pursued to the detriment of fundamental rights and democracy.

5.1. The concept of national security

The concept of security is used in different contexts where its scope varies depending on the threats in question.[64] We may thus distinguish external security, relative to threats originating outside a county's territory; internal security, relative to all threats to people's safety in a country or region, whatever their source; and global security, relative to threats that can only be addressed through transnational measures. For instance, the European Council characterises internal security as follows:

> *EU internal security means protecting people and the values of freedom and democracy, so that everyone can enjoy their daily lives without fear.*[65]

The Council lists the main threats to internal security as follows:

> *"terrorism, serious and organised crime, drug trafficking, cybercrime, trafficking in human beings, sexual exploitation of minors and child pornography, economic crime and corruption, trafficking in arms and cross-border crime," and moreover "violence itself, natural and man-made disasters,"*

[64] The term *security* derives from the Latin *securitas*, i.e., the state of being *securus*. In its turn, *securus* is composed of *se*, a prefix meaning "without," and *cura*, meaning "worry" or "care." Thus, being in a state or security originally meant being without care, worry, or anxiety, and, by extension, being without any danger or being adequately protected against any possible threat. When considered as an activity rather than as a condition, security is the activity carried out to prevent or counter such threats so as to ensure a condition of security.

[65] European Council. Internal security strategy for the European Union Towards a European security model. Publications Office of the European Union, 2010.

> *and other "other common phenomena which cause concern and pose safety and security threats to people across Europe, for example road traffic accidents"*

The notion of national security has a more restricted scope than internal security, covering challenges to the existence and integrity of a nation. Thus, we might say that national security is affected where a nation's fundamental interests are harmed or threatened, and that national security activities are meant to prevent such harm and deflect such threats. Originally, this notion was mainly used to address issues pertaining to the territorial integrity and political autonomy of nation-states, including interference by foreign powers, but also terrorism and violent subversion. Thus, security appeared to be connected to the idea of national defence, even though it included activities aimed at protecting against not only foreign but also to internal (violent) threats to the political community as a whole.

A definition to that effect can be found, for instance, in US law:[66]

> *National security refers to those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism.*

Broader notions of national security have been proposed that take the concept outside its original focus, to include all threats to a state's power (its sovereignty) and its ability to police its territory:

> *International terrorism is not the only threat stipulated by Western states in their national security outlooks. The range of orthodox threats remains part of their risk assessment. This includes transnational crime, weapons of mass destruction, conflicts within and between failed states, the outbreak of conventional warfare between advanced militaries and pandemics. In addition, a range of qualitatively 'new' threats are becoming recognized and taken into the 'security' portfolio, including climate change, poverty, water, energy and food security and technology failures in critical infrastructure.*[67]

For instance, the EU's security strategy mentions the following main security issues: the proliferation of weapons of mass destruction, terrorism and organised crime, cybersecurity, energy security, and climate change.[68]

This expanded notion of national security should be used with care and applied in a context-sensitive way. On the one hand, it may be useful to expand the scope of "national security" to implicitly extend the urgency that is usually associated with national defence and protection against terrorism to other critical domains of state action, such as climate change policy. On the other hand, this expansion may have unwanted side effects, since the concept of national security also provides a ground for limiting fundamental rights and other legal protections. If a constitutional system permits fundamental rights to be restricted for national security purposes or excludes certain legal constraints from being applied to national security activities, then —by applying an extended concept of national security indistinctively across the board— we risk expanding the state's power to restrict fundamental rights and to act without legal constraints. To prevent an excessively expansive use of the notion of *national* security, this notion should be carefully distinguished from the concept of *internal* security, the latter having a broader scope, including the prevention of risks to citizens, and in particular the enforcement of criminal law.

---

66 5 CFR § 1400.102 - Definitions and applicability.

67 Legrand, T. "National Security and Public Policy: Exceptionalism Versus Accountability." In *The Palgrave Handbook of National Security*. Ed. by Michael Clarke et al. 2022, pp. 53–72.

68 General Secretariat of the Council. European Security Strategy. A Secure Europe in a Better World. 2009.

The issue of how broad a notion of national security should be is indeed bound up with the "exceptionalism" that in this domain is often granted to state action. This "exceptionalism" should not be understood as the ability to suspend the rule of law (and the law itself) so as to preserve a national community,[69] as would be possible under an authoritarian interpretation of the principle that "the safety of the people is the supreme law."[70] It is rather to be understood as the possibility of restricting the scope of certain fundamental rights no more than is necessary to preserve a democratic community (whose preservation includes maintaining its democratic institutions and the rights of its citizens) from serious risks, and doing so within a legal framework.

However, it remains true that national security activities, even within a democratic constitutional order, require special consideration, since limitations and controls that are applicable in other domains may not be suitable, given that covert and timely interventions may be needed to counter certain serious risks (such as terrorist attacks).[71] Thus specific measures need to be put in place in order to ensure that individual rights and democratic principles are not unduly restricted and that secret services do not become a "state within a state" exempt from all legal constrains: greater focus on a precise legal framework, ex ante authorisation and ex post control by independent bodies, effective standards requiring all interferences to be based on evidence of serious threats, ex post notification to the affected individuals, and access to judicial remedies, consistency with human rights principles.

5.2. National security as a real or purported justification

It is often claimed that threats to national security have become more complex, unpredictable, and alarming, which justifies taking extreme measures to counter them. However, describing the current level of danger as "unprecedented" may be excessive, since events capable of claiming lives on a massive scale (e.g., pandemics such as the black death, which by some estimates killed half the European population) are a feature of every age. Certain threats have become undoubtedly more sophisticated (e.g., terrorist attacks), but so have the means by which we can address such threats and make societies more resilient.

Even discounting excessive alarms, it remains true that the need to protect national security may justify measures that entail serious restrictions of citizens' fundamental rights, as long as such measures are proportionate and necessary to preserve a democratic society. As we shall see, this is recognised by both the European Court of Human rights and by the European Court of justice (see Sections 6.2 and 7.2).

According to the EU Agency for Fundamental Rights the concept of national security has a broad and not clearly delimited meaning:[72]

---

[69] As in the approach developed by German Jurist Carl Schmitt, whose work contributed to legitimising Fascist governments: Schmitt, C. *Political Theology*. MIT, 1985 [1922].

[70] This motto—from the Latin *salus populi suprema lex*—goes back to Cicero's *On Laws* (*De Legibus*), bk. III, pt. III, sub. VIII.

[71] See: Auriel, P., Beaud, O., and Wellman, C. *The Rule of Crisis Terrorism, Emergency Legislation and the Rule of Law*. Springer, 2018.

[72] EU Agency for Fundamental Rights. Surveillance by intelligence services: *Fundamental rights safeguards and remedies in the EU. Volume II: Field perspectives and legal update*. Publications Office of the European Union, 2017.

> *[In] the ECtHR case law on national security [...] the latter goes beyond the protection of the territorial integrity of a state and protection of its democratic institutions – extending to major threats to public safety and including cyber-attacks on critical infrastructures.*

This should not, however, be understood as implying that states can label any initiatives they undertake as pertaining to national security, in such a way as to provide such initiatives with a legal and moral justification. There is indeed strong evidence, coming from different countries, including some Member States, that spyware is often misused, serving completely different purposes under the pretence of its necessity for national security.

The UN Human Rights Council has indeed recognised that many states have used antiterrorism powers as a cynical legal pretext to curtail freedom of expression, legitimise torture and other ill-treatment, and exert a chilling effect on minorities, activists, and political opposition. More specifically, the UN Special Rapporteur has made the following statement on appeals to national security being used to legitimise human rights abuses:

> *Many States have adopted laws that loosely invoke national security, national interest or public order as all-encompassing categories that often include any act criminalized solely through the subjective lens of the impact that it may have, including those "affecting national security, political and social stability" and "dangerous to the political, economic or social system." Many activities of civil society organizations, human rights defenders, journalists, bloggers and political opponents will fall under such laws, whose main objective is to criminalize legitimate expressions of opinion and thought.* [73]

Even the National Security Agency (NSA) report prepared by the Obama administration[74] states that national security should never be invoked to justify certain interferences with individual rights and social values:

> *Some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.*

A strong denunciation of abusive appeals to national security has been put forward by the European Commissioner for Justice Didier Reynders. Speaking to the European Parliament in September 2021, he has indeed "totally condemned" alleged attempts by national security services to illegally obtain information on political opponents through their phones. He stated that "any indication that such intrusion of privacy actually occurred needs to be thoroughly investigated and all responsible for a possible breach have to be brought to justice."[75]

The previously mentioned Pegasus Project, an international investigative journalism initiative,[76] has provided extensive evidence on Pegasus being used to target individuals— such as political opponents, human rights activists, lawyers, and journalists— who do not have any connection to serious crimes and pose no national security threats. As noted above, evidence of Pegasus attacks has

---

[73] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2019). *Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders.* Delivered to the 40th session of the Human Rights Council.

[74] Clarke, R. A. et al. *The NSA Report, Liberty and Security in a Changing World.* Princeton University Press, 2014.

[75] Boffey, D. EU Commissioner calls for urgent action against Pegasus spyware. In:*The Guardian* (2021 - 15 September).

[76] Forbidden stories, https://forbiddenstories.org/.

been found in the phones of more than 300 people, among whom more than 100 political activists, lawyers, and journalists (see Figure 9).[77] Many such spyware operations are likely to be mainly or solely motivated by illegitimate goals, such as interfering with the victims' lawful activity and subjecting them to blackmailing, attacks, and sanctions.[78] Such operations (and the measures authorising them) are unlawful under fundamental/human rights law, since they cannot be shown to be connected to an interest which might justify restricting the affected rights. It is true that both the right to private life and the right to freedom of expression may be subject to lawful restrictions in the interest of national security, but this should only be the case when the restrictive measures actually pursue national security. When the pursuit of national security is only a pretence, the restrictions allegedly motivated by it obviously remain unlawful.[79]

Figure 9: Who has been targeted by Pegasus[80]

[77] Forbidden stories. https://forbiddenstories.org/pegasus-project-impacts-map/ (accessed on 11 December 2022).

[78] Forbidden stories. https://forbiddenstories.org/pegasus-journalists-under-surveillance/.

[79] With regard to freedom of expression, see: Human Rights Committee. General comment No.34 on Article 19: Freedoms of opinion and expression. United Nations. CCPR/C/GC/34, 2011, paras. 29-32.

[80] BBC News, 22 July 2021, https://www.bbc.com/news/world-57891506.

6. PEGASUS AND INTERNATIONAL HUMAN RIGHTS LAW

KEY FINDINGS

In the UN framework, surveillance activities are to be assessed according to human rights treaties such as the International Covenant on Civil and Political Rights. Abusive surveillance affects not only the rights to privacy but also freedom of expression and other rights in the Covenant. Both privacy and freedom of expression can only be limited through the law, and as necessary for the indicated purposes. National security may justify limitation, but in the case of Pegasus, the legality and necessity requirements are likely not satisfied.

Also applying to targeted surveillance is the framework of the European Convention on Human Rights, specifically through its requirements of legitimacy, legality, necessity, and proportionality in the context of a democratic society. An extensive case law of the European Court of Human Rights has set conditions for covert surveillance to be consistent with human rights, particularly with regard to legality (accessibility of the laws authorising surveillance and foreseeability of their consequences) and notification. The Court has also granted standing to individuals only potentially affected by covert surveillance.

In this section we examine the extent to which spyware such as Pegasus may comply with international human rights law. We will first consider the UN framework and then move on to the European Convention on Human Rights.

6.1. The UN framework

In the UN framework, surveillance activities are to be assessed having regard to the Universal Declaration of Human Rights and the relevant human rights treaties, such as the International Covenant on Civil and Political Rights, which has been ratified by all Member States.

The broadest guarantee against abusive surveillance is provided by the right to the protection against interference with "privacy, family, home or correspondence" and attacks on "honour and reputation" (Art. 17 of the Covenant). This right is interfered with where information is collected from an individual device, transmitted to others, and further processed without the individual concerned consenting to, or even knowing of, these operations. It is also violated when the collected information is used, and possibly manipulated, to undermine the reputation of the targeted individuals.

Other rights and principles come to the fore as well, such as freedom of opinion and expression, including the freedom to "hold opinions" and "seek, receive and impart information and ideas" (Art. 19). Freedom of expression is violated when individuals, suspecting or being aware that they may be subject to surveillance, consequently, feel they must refrain from expressing their opinions (e.g., by using their devices in communications) or seeking information (e.g., in accessing online content).

The right to due process (Art. 14) is also at play. It is so whenever the individuals concerned are not duly informed that they have been subject to surveillance measures or have no possibility to access a court having the jurisdiction or the resources to effectively address their complaints. Similarly, the presumption of innocence may be affected where targeted individuals are unjustly accused on the basis of partial, misleading, or manipulated information collected about them, or even on the basis of

false evidence planted on their devices. Where —as has often been the case with the use of Pegasus— political activists and candidates are targeted, the threat also affects the right to "take part in the conduct of public affairs, directly or through freely chosen representatives" and the right "to vote and to be elected" (Art. 25).

Spyware may also affect other rights in the Convention, such as the guarantees of peaceful assembly (Article 21) and association (Art. 22), and non-discrimination obligations (Articles 2(1), 4(1), and 26). Adverse activities triggered by the information collected through the spyware may also violate other protections, such as the right to life (Art. 6), the prohibition on torture (Art. 7), freedom from arbitrary detention (Art. 9), the right to freedom of movement (Art. 12), and due process (Art. 14).

The lawfulness of restrictions on the rights contained in the Universal Declaration is addressed in Art. 29, according to which

> *everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society*.

More specific conditions under which civil and political rights may be limited are indicated in the Covenant. In particular, the freedom of expression can only be limited *by law and to the extent that it is necessary*," "for respect of the rights or reputations of others" or for "the protection of national security or of public order (*ordre public*), or of public health or morals" (Art. 19). The same idea is expressed in relation to the rights to assembly and association (Arts. 21 and 22), where it is specified that the necessity must be relative to a *democratic society*.

Both the Human Rights Committee and the General Assembly have affirmed the need to ensure the protection of human rights in the context of state surveillance. The Human Rights Committee[81] has observed that the right to privacy requires that robust and independent oversight systems be in place regarding surveillance, interception, and hacking.[82] The General Assembly[83] has noted that surveillance of digital communications must be consistent with international law, and it stated that "any interference with the right to privacy should take into account its legality, necessity and proportionality."

UN special rapporteurs have repeatedly underscored the need to rigorously assess surveillance interferences with fundamental rights. The Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has emphatically stated that surveillance, including for the purpose of national security, should be restricted and surrounded by legal safeguards:

> *Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law*.[84]

---

81 Human Rights Committee. General comment No. 34 on Article 19.

82 United Nations. Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. A/HRC/34/60, 2017.

83 United Nations, General Assembly. The right to privacy in the digital age: resolution. United Nations. A/RES/73/179, 2019.

84 United Nations. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/23/40, 2013.

Moreover, "individuals should have the right to be notified that they have been subjected to communications surveillance" and should "have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath."

The Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression[85] has observed that surveillance activities, including in particular computer interference and mobile-device hacking, must respect the principles of legality (requiring the activity to be authorised by sufficiently precise and unambiguous legal rules), necessity (the least restrictive means should be used to achieve the purpose), proportionality (the advantages to national security should not be outweighed by the disadvantages or detriment to individual rights), and, moreover, legitimacy (the restriction must be intended to achieve those goals for which such a restriction is allowed, namely, in our case, national security). This last criterion means that national security, if it is to justify limitations on privacy and freedom, must be understood properly, i.e., as only concerning "situations in which the interest of the whole nation is at stake," as when a state's political independence and territorial integrity" is at issue. Thus, the requirement of legitimacy rules out the possibility of invoking national security to justify restrictions "in the sole interest of a government, regime or power group."

The final recommendations by the Rapporteur include the following:[86]

- States should impose an immediate moratorium on the export, sale, transfer, use, or servicing of privately developed surveillance tools until a regime is in place for ensuring compliance with human-rights safeguards.
- States that purchase or use surveillance technologies ("purchasing States") should ensure that domestic laws permit their use only in keeping with human rights standards, and they should establish legal mechanisms of redress.

The proposal of a moratorium on spyware has so far been endorsed only by Costa Rica.

These conclusions have been reiterated in testimony delivered to the EU Parliament by Mr. Kaye, UN Special Rapporteur on Freedom of Opinion and Expression from 2014 to 2022. He testified that the deployment of Pegasus fails to satisfy the conditions required for a lawful restriction of human rights (especially under Arts. 17 and 19 of the convention), since Pegasus allows indiscriminate access to a device's data and recording functions, making it impossible to ensure that only information that is necessary for a legitimate interest is collected.[87]

Mr. Kaye has also observed that state immunity should not be invoked to shield states and their officers from liability for use of spyware outside their territory:

> *[F]oreign sovereign and official immunities should not apply to protect state or non-state actors responsible for targeting individuals with spyware across borders. This is in part because states have an obligation to take positive steps to protect the enjoyment of individual rights and remedies.*[31]

[85] United Nations. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. A/HRC/41/35, 2019.

[86] United Nations. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, para. 66.

[87] Kaye, David. *The impact of spyware on fundamental rights.* Testimony to the PEGA Committee of the European Parliament, 27 October 2022.

6.2. The framework of the European Convention on Human Rights

The European Court of Human Rights has found that secret surveillance encroaches on "private life," but also sometimes on the "home" and on "correspondence," and so an issue arises under Article 8 of the Convention.[88]

Such an interference may be justified only as long as the conditions specified in Article 8 (2) are satisfied, i.e., when the interference

> *is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others* [...].

Accordingly, the covert use of spyware in the context of national security operations is only admissible where it effectively pursues national security goals —thus meeting the standard of *legitimacy*— and moreover it meets the standards of *legality* and *necessity in a democratic society*.

As to the question of whether a measure really pursues national security goals, the Court has recognised that Member States have a margin of appreciation in determining what objectives contribute to national security and what means are best suited to achieving such objectives. However, the enjoyment of this margin of appreciation is subject to supervision.[89] Considering that it may not be well equipped to challenge the judgment of national authorities in such matters, the Court requires that in the event of any alleged threat to national security being used as a ground for restricting a human right, independent national bodies be authorised to verify, by means of some form of adversarial proceedings, that the threat has a reasonable basis in fact.[90]

On the standard of legality, the Court has specified that a surveillance measure "must have some basis in domestic law and, with regard to the quality of the law at issue, it must be accessible to the person concerned and have foreseeable consequences."[91] It has to "indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."[92] The Court has further developed a set of minimum requirements for the law to meet in order to avoid abuses of power: "the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances under which recordings may or must be erased or destroyed."[93]

As concerns necessity in a democratic society, a measure may fail to satisfy this requirement when either (a) less restrictive measures could have been adopted, possibly by taking additional precautions

---

88 European Court of Human Rights. *Guide to the Case-Law of the European Court of Human Rights. Data protection*. Council of Europe Publishing, 2022.

89 Handyside v. the United Kingdom, cited above, para. 49.

90 Janowiec and Others v. Russia [GC] (nos. 55508/07 and 29520/09, 21 October 2013).

91 Kennedy v. the United Kingdom (no. 26839/05, 18 May 2010).

92 Kennedy v. the United Kingdom, para. 230.

93 Kennedy v. the United Kingdom, para. 231.

and implementing controls, or (b) the interference with the rights of the individual concerned is so serious that it outweighs whatever benefit the measure may bring to national security.

According to the Court, "the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued." Thus, even though national authorities enjoy a margin of appreciation in matters of national security," "the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life." [94] In subsequent cases, the Court held that covert surveillance should only be tolerated when "strictly necessary." [95]

An important development in the case law of the ECtHR pertains the conditions under which a person has standing in front of the Court, so that their case can be examined. While the individuals concerned usually need to provide evidence that their rights have been directly affected, the ECtHR has held than victim status can be recognised —and standing can consequently be granted— even if such individuals cannot prove that covert surveillance measures have been specifically applied to them. It is sufficient that evidence is provided that secret surveillance measures are currently in place or that legislation exists permitting such measures, and that effective national remedies are not available.

> *the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies.* [96]

To ensure access to effective remedies, the ECtHR has introduced a strict notification requirement: the individuals targeted with a covert surveillance measure need to be notified of such a measure, "[a]s soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measure."[97] Timely notification is indeed "inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers."[98]

Finally, the European Court of Human Rights has considered the connection between surveillance and freedom of expression in relation to journalism. In various cases, the Court has sanctioned access to confidential journalistic material in bulk-interception regimes.[99] These cases highlight the key importance of protecting journalism in the framework of the Convention, though addressing mass surveillance, rather than targeted surveillance through spyware. However, in other cases, the Court has focused on individualised surveillance in ways similar to what is enabled by Pegasus, though in a simpler technological environment. For instance, Court unanimously held that Azerbaijan violated the right to privacy and freedom of expression in a case in which a journalist was put under covert

---

94 Leander v. Sweden (no. 9248/81, Series A, 26 March 1987), para. 59.

95 Malone v. the United Kingdom (no. 8691/79, Series A, 2 August 1984).

96 Roman Zakharov v. Russia (no. 47143/06, § 171), ECHR 2015.

97 Roman Zakharov v. Russia, para. 287.

98 Roman Zakharov v. Russia, para. 234.

99 Big Brother Watch and Others v. the United Kingdom (nos. 58170/13 and 2 others), §§ 447–50, 25 May 2021.

surveillance: wires and hidden cameras were installed in her house, intimate videos were recorded of her in her bedroom and then disseminated online, a threatening letter was sent to her, and sensitive personal information about her was disclosed in an investigative report; all these actions were allegedly part of an intimidation campaign.[100] Note that in order to establish the responsibility of Azerbaijan, it was not necessary to prove that officers of the state had directly engaged in, or organised, the surveillance, since the Court held that Azerbaijan violated its positive obligation under Art. 10 to protect the journalist's freedom of expression.

Some novel cases dealing with surveillance are currently being examined by the European Court of Human Rights. On 27 September 2022, a Chamber hearing was held in a case by a lawyer and four human right activists concerning a claim based on Article 8 of the Convention (right to private life).[101] The applicants claimed that Polish law permitted police and intelligence services to monitor their telecommunications and digital communications without their knowledge. Moreover, they argued that they had no effective remedies under Polish law, since these services were not required to inform the targeted individuals about surveillance measures directed at them. Therefore these measures could not be subjected to judicial review.

[100] Khadija Ismayilova v. Azerbaijan (no. 65286/13 and 57270/14, 10 January 2019).

[101] Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland (nos. 72038/17 and 25237/18).

7. PEGASUS AND EU LAW

KEY FINDINGS

In the context of EU law, targeted surveillance is relevant to the rights enshrined in the Charter of Fundamental Rights of the European Union, the principles set forth in the Treaties (such as democracy and the rule of law), and various instruments of EU secondary law, such as those pertaining to data protection law.

According to the Treaty on European Union, national security is the sole responsibility of each Member State. This does not in principle exclude that national security activities are subject to EU law when they interfere with activities regulated by EU law.

However, the application of EU law to the use of spyware for national security purposes is hindered by the fact that national security activities are excluded from the scope of two fundamental instruments, the GDPR and the ePrivacy Directive. This limitation to the protection of data subjects relative to state activity can hardly be justified with regard to the rights contained in the Charter and the principles contained in the Treaties. Because this exclusion may be used too broadly, it needs to be pointed out that it only concerns cases in which the spyware is genuinely designed to protect national security properly understood.

EU law applies to the use of covert investigations for law enforcement purposes, which are subject to the Law Enforcement Directive. However, even in this domain evidence exists of abusive national practices.

In this section we will consider the relationship between measures adopted by Member States for national security and EU law, with a focus on data protection.

7.1. Spyware and national security in the EU Treaties

The use of spyware to achieve national security goals is subject matter that falls within the scope of many provisions of EU law contained in the Treaties and in the Charter. This is due to the fact that, as just noted, the mere possibility of being put under pervasive observation (and being consequently exposed to adverse actions) precludes autonomous action in the individual, cultural, and political spheres.

There is a whole range of rights and principles that surveillance interferes with. We previously discussed the UN Covenant on Civil and Political Rights and the European Convention on Human Rights as standards against which such interference may be assessed. But we can importantly also turn to the Charter as a standard, which, as just hinted at, contains a pertinent list of rights and principles as follows:

- The principle of dignity (Art. 1).
- The right to liberty and security (Art. 6).
- The rights to private life and data protection (Arts. 7 and 8).
- Freedom of thought, conscience, and religion (Art. 10).

- Freedom of expression and information, including the freedom of the media (in particular where journalists are targeted) (Art. 11).
- Freedom of assembly and association (Art. 12), including the freedom to join political parties (Art. 12(2)).
- Freedom of the arts and of scientific research and academic freedom (Art. 13).
- The right to property (Art. 17), especially where, as in the case of Pegasus, the surveillance involves access to individual property.
- The right to non-discrimination (Art. 21), where surveillance or consequent actions are specifically directed against individuals belonging to particular groups, as identified, e.g., by their holding certain political views.
- The right to engage in collective action (Art. 28), where workers and their organisations are targeted.
- The right to stand as a candidate in European and municipal elections (Arts. 39 and 40), where individuals who hold political positions or aspire to hold them are targeted, thereby affecting participation in elections or the fairness of the electoral process.
- The right to an effective remedy and to a fair trial (Art. 47), where the targeted individual has no effective remedy at their disposal against unlawful surveillance.
- The presumption of innocence (Art. 48), where the collected information is used to make false accusations, and where control over devices is used to fabricate false evidence.

Two general provisions of the Charter are also relevant to our analysis. According to Art. 51, the application of the Charter is limited to the implementation of Union law:

> *The provisions of this Charter are addressed* […] *to the Member States only when they are implementing Union law*.

According to Art. 52(1), all limitations on the rights and freedoms established by the Charter must satisfy the principles of legality and proportionality (including the need to pursue objectives of general interest). Thus, each such limitation must (*i*) be established by law, (*ii*) contribute to an objective of general interest or to the protection of the rights and freedoms of others, (*iii*) be necessary for that objective, and (*iv*) be balanced (the objective of surveillance must be pursued in such a way that the benefits are not outweighed by the detriment resulting from adverse interference with those rights and freedoms):

> *Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*.

Finally, according to Art. 52(3), the rights contained in the Charter are assumed to coincide, in their meaning and scope, with the corresponding rights in the European Convention on Human Rights, meaning that the previous analysis, developed relative to the Convention, is also significant for the Charter.

Pervasive surveillance interferes not only with individual rights but also with the fundamental values of democracy and the rule of law, since the infringement of individual rights directly affects the

implementation of such values (see Section 4), which are listed in Art. 2 of the consolidated version of the Treaty on European Union (TEU):

> *The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights.*

By interfering with the political engagement of individuals —and in particular of those who hold or are interested in holding public office— unlawful surveillance undermines the principle of representative democracy, which under Art. 10(1) TEU stands as the foundation of the functioning of the Union:

> *The functioning of the Union shall be founded on representative democracy.*

In the TEU, national security is specifically addressed in Art. 4:

> *The Union shall respect* [... the Member States'] *essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.*

Thus, the EU is bound to respect national security as an essential state function, which remains the sole responsibility of each Member State. As a consequence of this provision, a potential tension emerges between, on the one hand, a state's power to engage in national security activities as they choose (as set forth in Art. 4) and, on the other hand, the need to preserve EU fundamental rights and values when these are adversely affected by state activities ostensibly aimed at preserving national security.

The general issue we need to address is whether from the fact that a competence, or power, has not been transferred to the EU, it follows that a state can freely act in exercising such competence, even when its behaviour violates EU norms, rights, and principles. In other terms, we need to ask whether the fact that a state measure is carried out under a non-transferred competence (a power not reserved to the EU) entails that EU law does not apply to that measure. We can distinguish state competences not yet transferred to the EU (retained competences) and competences which the Treaty explicitly reserves to Member States (reserved competences), such as national security.[102]

Certainly, the fact that a competence has not yet been transferred to a Member State does not entail that the acts performed in exercising that competence are excluded from the scope of EU law. This principle was affirmed by the ECJ in a variety of cases, an example being *Schwarz*, concerning taxation of educational activities. The Court stated that

> *although direct taxation falls within their competence, the Member States must none the less exercise that competence consistently with Community law* [...] *in particular the provision on the freedom to provide services.*[103]

A similar analysis also applies to the activities that pertain to competences reserved to Member States, such as national security. The assessment of the permissibility of national security measures under EU law is not meant to impose on the states concerned particular ways to achieve their national security purposes (as this would violate the states' reserved competences), but rather to determine whether such measures are compatible with the principles, rights, and rules of EU law within domains governed by EU law. When such measures interfere with fundamental rights, this determination requires a legality and proportionality assessment, ultimately to be performed by the ECJ.

---

[102] Following De Witte, B. "Exclusive Member State Competences: Is There Such a Thing?" In *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future.* Hart, 2017, pp. 59–73.

[103] Judgment of 11 September 2007, *Schwarz and Gootjes*, C-76/05, ECLI:EU:C:2007:492, para. 69.

This assessment, however, presupposes that the interference takes place within the scope of EU law, since the Charter, too, is to be applied "to the Member States only when they are implementing Union law" (Art. 51).

However, the conclusion that a certain state activity (or the activity by a private party requested by a state) may justify restricting EU fundamental rights or may even be excluded from certain EU legal instruments, on the ground that it pertains to national security presupposes that that the activity in question is classified as pertaining to national security. We submit that this preliminary issue, pertaining to the qualification of nature of the state activities, necessarily pertains to EU law, and therefore falls within the competence of the ECJ. The EU law notion of national security —while accommodating different national evaluations relative to what serious threats most endanger a national community— certainly cannot include activities aimed at targeting political opponents or minorities.

7.2. The Court of Justice on fundamental rights, data protection, and national security

The Court of Justice has examined the connection between fundamental rights and national security in some important cases.

Among them, we will just mention the *Schrems I* and *Schrems II* cases,[104] where the Court respectively invalidated the Safe Harbour agreement and the subsequent Privacy Shield (on the transmission of personal data from the EU to US). A key ground for these holdings was the fact that the data transferred to the US would be processed by US national security agencies, without the constraints and remedies in place in the EU (and so in violation of the right to data protection and of the right to an effective remedy). In *Schrems II*, the Court found that the US regulation of surveillance for the purpose of national security did not meet

> *the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary*.[105]

On the right to an effective remedy the Court stated that

> *legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection* [...].[106]

In the 2020 *Quadrature du Net* case,[107] the ECJ considered a French law requiring communications service providers to retain traffic data. It stated that Article 15 of the ePrivacy Directive, interpreted according to the Charter, precludes legislative provisions like the one being contested, i.e., provisions requiring, "as a preventive measure, […] the general and indiscriminate retention of traffic and location

[104] Judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (Schrems I), and Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (Schrems II).

[105] *Schrems II*, para. 184.

[106] *Schrems II*, para. 187.

[107] Judgment of 6 October 2020, *La Quadrature du Net and Others* v *Premier ministre and Others*, Joined Cases C-511/18, C-512/18, and C-520/18, ECLI:EU:C:2020:791.

data."[108] However, the Court recognised that for the purpose of countering serious threats to national security, providers of electronic communications services could be required to "retain, generally and indiscriminately, traffic and location data"[109] as long as this was only for a specific period of time, and under appropriate safeguards. It also recognised that providers could be required to engage in automatic analyses of traffic and location data in order to counter serious and actual threats to national security. Moreover, subject to prior independent review, even real-time collection of technical data on the location of a terminal equipment could be justified relative to individuals who are suspected to be involved in terrorism.

In the 2022 joined cases *SpaceNet* and *Telekom Deutschland*,[110] the Court of Justice confirmed that EU law precludes general and indiscriminate retention of traffic and location data on a preventive basis. However, in the case of a serious threat to national security such a general and indiscriminate retention is permissible for a limited time, under appropriate safeguards. Moreover, for the purpose of combating serious crime and safeguarding public security, the targeted retention of traffic and location data —in relation to the categories of persons concerned or using a geographical criterion— is permissible for a limited period.

Thus, the Court upheld a legal framework that, in keeping with legality and proportionality, recognises that significant restrictions of fundamental rights and data protection norms are permissible for the purpose of national security and to a lesser extent for combating serious crime and preserving public security.

7.3. National security and data protection in EU law

As noted in Section 5.1, the provisions of the Charter "are addressed […] to the Member States only when they are implementing Union law" (Art. 51). Thus, to determine to what extent the Charter applies to national security activities, we need to consider the extent to which such activities fall under EU law. If such activities are excluded from certain provisions of EU law, then there is no protection that can be granted under such provisions or under the Charter in connection with their interpretation and application.

This exclusion may have some paradoxical implications. For instance, if national security activities are completely excluded from the scope of data protection law, then the decisions issued by the ECJ in *Schrems I* and *II* would appear to be questionable: they would be based on standards —such as "minimum safeguards resulting, under EU law, from the principle of proportionality "— that the ECJ itself does not apply within the EU. In fact, in these decisions, the Court invalidated the schemes from the transmission of data from the EU to the US because US law did not provide a protection comparable to that granted by EU law with regard to the processing of personal data for the purpose of national security. If data protection law does not apply to national security activities, then the difference between the US and EU legal frameworks, relative to regulation of such activities, seems largely to disappear.

[108] Quadrature du Net, para. 168.

[109] Ibid.

[110] Judgment of 20 September 2022, *Bundesrepublik Deutschland* v *SpaceNet AG* (C-793/19) and *Telekom Deutschland GmbH* (C-794/19), ECLI:EU:C:2022:702.

Indeed, in presenting a draft report on Pegasus, the MEP Sophie in 't Veld pointed out that the EU may appear to be operating under a double standard with regard to digital threats to democracy: while the Commission is determined to fight attacks on democracy from the outside, when a threat to democracy comes from the governments of EU member states, it suddenly considers that the defence of European democracy is no longer a European matter but a matter for the Member States.[111]

To assess the extent to which data protection law is applicable to national security activities, we need to consider that the GDPR and the ePrivacy Directive contain two kinds of provisions that are relevant to the processing of personal data for the purpose of national security:

- exclusion provisions, according to which national security activities are not included from the scope of such instruments; and
- limitation provisions, according to which restrictions to the same instruments for the purpose of national security are permissible but only on condition that they meet legality and proportionality requirements.

Scope-limitation provisions

According to Art. 2(2) of the GDPR, the Regulation

> *does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law.*

Recital 16 explicitly states that the activities falling "outside the scope of Union law" include national security:

> *This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security.*

Similarly, Art. 1(3) of the ePrivacy Directive, states that the Directive

> *shall not apply in any case to activities State security (including the economic well-being of the State* […]*).*

Limitation provisions

According to art. 23 GDPR

> *Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard* [. . .] *national security* [. . .].

Similarly, Art. 15 of the ePrivacy Directive states that:

> *Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e., State security).*

[111] See Rankin, Jennifer. "Dutch MEP says illegal spyware 'a grave threat to democracy.'" In *The Guardian* (8 November 2022).

It may seem that these exclusion and limitation provisions cannot be reconciled: if national security activities are not included in the scope of the GDPR and the ePrivacy Directive, then it makes little sense to establish under what conditions rights and obligations established by such instruments may be restricted for the purpose of national security.

However, a reconciliation may be achieved by distinguishing between the purpose of certain data-processing activities and the purpose of the restrictions imposed upon the rights of obligations pertaining to such activities. The purpose of the data processing activities at stake —rather than the purpose of the restrictions— determine whether such activities are included in the scope of data protection law. For instance, the data retention requirements imposed on providers for the purpose of national security concern processing activities aimed at providing communications services, activities which fall within the ePrivacy Directive. Thus, such requirements have to be assessed according to the criteria established by Art. 15 of the Directive.

This is indeed the approach developed by the ECJ[112] relatively to both law enforcement[113] and national security[114]. According to the Court, the ePrivacy Directive must apply to measures imposed upon providers for purposes of law enforcement and national security, since Art. 15 (1) of the Directive explicitly regulates the lawfulness of measures restricting data subjects' rights for such purposes:

> *Article 15(1) of Directive 2002/58 necessarily presupposes that the national legislative measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.*[115]

Indeed, legislation imposing data retention measures upon providers, while being aimed at purposes pertaining to law enforcement or national security, still addresses the provision of electronic communication services. The latter activity is subject to the ePrivacy Directive, which governs

> *all operations processing personal data carried out by providers of electronic communications services [...], including processing operations resulting from obligations imposed on those providers by the public authorities*[116]

The considerations just developed against an exclusion of certain national security measures from the scope of data protection law, do not apply to the activities involving use of spyware by State officers —or by private contractors appointed by them— as long these activities genuinely serve national security purposes. They may however apply to cases in which communication service providers are ordered to cooperate with State authorities in the installation and use of spyware, so interfering with the services that such providers are delivering to their clients.

An important provision on the protection of media service providers and journalists has been included in the proposed Media Services Act, and in particular by Art. 4(2)(c), "Rights of Media Service Providers." According to this provision, Member States must not

> *deploy spyware in any device or machine used by media service providers or, if applicable, their family members, or their employees or their family members, unless the deployment is justified,*

---

[112] See Buchta, A. and Kranenborg, H. Institutional report topic 2: The new EU data protection regime. In *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection. The XXIX FIDE Congress in the Hague.* Eleven, 2020, pp. 79–105.

[113] Judgment of the Court of 21 December 2016, Cases C-203/15 and C-698/15, Tele2/Watson.

[114] Judgment of 6 Oct 2020, C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others.

[115] Ibid., para. 95.

[116] Ibid., para. 101.

> *on a case-by-case basis, on grounds of national security and is in compliance with Article 52(1) of the Charter and other Union law*

This provision requires that each deployment of spyware for such purposes be assessed on the basis of proportionality according to Art. 52 of the Charter. It also ensures that the European Convention on Human rights applies, as referred to by the Charter.

7.4. The use of spyware for the purpose of law enforcement

While national security activities are excluded from the scope of key instruments of EU data protection law, this is not the case for law enforcement activities.[117] The latter activities fall under the Law Enforcement Directive (LED),[118] which under Art. 1(1) governs

> *the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*

Such processing is only lawful (Art. 8)

> *if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.*

Moreover, the processing at stake must satisfy the data protection principles (lawfulness, fairness, minimisation, accuracy, security, etc.) mentioned in Art. 4.

Covert investigations are not excluded by the Directive. However, according to Recital 26, such investigations can only be done

> *as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned.*

Thus, the Charter —with the conditions it sets for restricting fundamental rights— fully applies to such investigations and to the measures authorising them, as stated in Recital 46:

> *Any restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.*

In determining whether the use of Pegasus may be consistent with the Directive and with the Charter, we need to consider if the requirements of both the Directive (and the Charter) are all satisfied.

The permissibility of using Pegasus —and similar device-hacking systems— for law enforcement purposes needs to be considered case by case, taking account of multiple factors: the seriousness of

---

[117] On device hacking in the context of law enforcement, see: Gutheil, M., Liger, Q., Heetman, A., Eager, J., and Crawford, M. *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices. Study requested by the LIBE committee*. European Parliament, 2017.

[118] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ("LED") (OJ L 119, 4.5.2016, p. 89).

the crime or security risk to be investigated or prevented, the constraints under which the system's functionalities are used, and the applicable national law. However, it seems that Pegasus would not be likely to meet the necessity requirement, under both the Directive and the Charter, as long as alternatives exist that achieve the law enforcement purposes in less intrusive and more secure ways.[119]

The implementation of legality principle in national law also has to be carefully scrutinised so as to determine the lawfulness of covert investigations. For instance, the Venice Commission, in its 2016 Opinion on the Amendments to the Polish Police Act,[120] has concluded that

> *the procedural safeguards and material conditions set in the Police Act for implementing secret surveillance are still insufficient to prevent its excessive use and unjustified interference with the privacy of individuals.*

Moreover, it has been observed that Polish law explicitly exempts from the scope of the Law Enforcement Directive the activities of the Polish Central Anticorruption Bureau, whose activity at least partly pertains to law enforcement,[121] and which therefore falls within the scope of the Law Enforcement Directive.[122] It may consequently be argued that this exemption constitutes an incorrect transposition of LED provisions into Polish law and is therefore contrary to EU law.

More generally, the question of whether an activity pertains to law enforcement —for the purpose of determining whether it falls under the Directive— has to be answered on the basis of EU law (Art. 1 of the Directive). Thus, if state law classifies as pertaining to national security an activity that according to Art. 1 instead concerns law enforcement, the first classification should be inapplicable for the purpose of the application of the Directive, so that the activity will remain subject to the rules governing law enforcement according to (the transposition) of the Directive.

---

[119] On Pegasus and law enforcement, see Vogiatzoglou, P., Marquenie, T., and Valke, P. *Assessment of the Implementation of the Law Enforcement Directive. Study requested by the LIBE committee.* European Parliament, 2022.

[120] Opinion on amendments to the Act of 25 June 2015 on the Constitutional Tribunal of Poland, adopted by the Venice Commission at its 106th Plenary Session (Venice, 11–12 March 2016). The Venice Commission, officially the European Commission for Democracy through Law, is an advisory body of the Council of Europe and is composed of independent experts in constitutional law.

[121] Litwiński P. *Opinia prawna w sprawie naruszeń, w związku z ujawnionymi przypadkami użycia oprogramowania szpiegującego Pegasus w świetle prawa ochrony danych osobowych, przepisów Karty Praw Podstawowych UE i Konstytucji RP*, Kancelaria Senatu, Warszawa 2022, https://www.senat.gov.pl/gfx/senat/pl/senateksperty zy/6283/plik/oe-390.pdf

[122] Litwiński P. *Opinia prawna w sprawie naruszeń*.

8. THE WAY FORWARD

KEY FINDINGS

The use of spyware poses a threat to the fundamental rights and basic principles of EU law, such as (representative-deliberative) democracy and the rule of law. It risks undercutting the very principles on which the EU legal system is based.

National security activities, in the international and European legal systems, can justify restrictions of fundamental rights, but if such restrictions are to be lawful, they need to satisfy the conditions of *legitimacy*, *legality, necessity*, *balancing*, and *consistency with democracy*.

In many instances of its deployment, Pegasus has so far failed to meet these requirements, given that it has been used for non-legitimate purposes, without an adequate legal framework, in the absence of real necessity, and causing disproportionate harm to individual rights and democracy.

We suggest various ideas that may help prevent abuses:

- Circumscribing the material scope of national security activities so as to make it more difficult for states to use national security as a spurious legal justification for activities directed at other purposes.
- Circumscribing the personal scope of national security activities, excluding from it certain activities by private parties.
- Including national security activity within the scope of data protection law so as to ensure that restrictions of data subjects' rights for national security purposes are subject to requirements of legality and proportionality.
- Supporting the adoption of adequate legal frameworks at the national level, since national security remains a reserved competence of Member States, and it is up to them to effectively ensure that their activity complies with the fundamental rights and principles of EU law. These frameworks should comply with such principles as the following: legality, legitimate end, necessity, proportionality, competent authority, due process, user notification, transparency, public oversight, security and certification, and technical adjustability.

A politically feasible moratorium on the use of device-hacking tools could consist in a strong presumption against the lawfulness of their use, a presumption grounded in the extensive evidence of their abusive deployments. This presumption could only be overcome when a state convincingly shows a willingness and capacity to prevent all abuses.

Moreover, Member States should be urged to ban the use of specific spyware tools, where, as in the case of Pegasus, there is strong evidence of their deployment in unlawful activities, especially within the EU. Until there is clear evidence that such unacceptable practices no longer take place, continuing to deploy Pegasus, even within the framework of lawful activities, entails supporting its producers and developers and thus implies a political (even if not a legal) complicity with such practices.

We have argued that the use of spyware poses a threat to the fundamental rights and basic principles of EU law, such as (representative-deliberative) democracy and the rule of law. It risks undercutting the very principles on which the EU legal system is based. In this section we will summarise the conditions for the lawful deployment of spyware and will bring them to bear on the Pegasus case.

8.1. Lawful restrictions of fundamental rights for national security purposes

National security activities, in the international and European legal systems, can justify restrictions of fundamental rights, but if such restrictions are to be lawful, they need to satisfy all of the following conditions:

- *Legitimacy*. The activities at issue must be aimed at genuine national security goals.
- *Legality*. They need to have a solid legal basis, that is, there must be laws on which they are based, and the language of these laws must be sufficiently clear and precise.
- *Necessity*. It must be the case that no better way exists to achieve the same national security goals, i.e., that all other means are either more infringing (resulting in a greater encroachment on rights) or less effective (failing to achieve national security goals to an equal or greater extent).
- *Balancing*. The importance of achieving the national security goals must not be outweighed by the negative impacts on the affected rights and values.
- *Consistency with democracy*. The pursuit of national security goals should contribute to preserving democratic societal arrangements, rather than undermining democratic processes.

The need for such standards to be met in national security activities can be extracted from UN sources, as well as from the European Convention on Human and the European Treaties and the Charter, whose provisions are to be interpreted consistently with the Convention.

It is not easy to reconcile the use of Pegasus with these requirements.

- In many cases it appears to have been used to pursue goals that do not concern national security, understood as protection of society as a whole.
- The pervasive surveillance it provides is not governed by an adequate legal framework.
- In most of these cases, it would have been possible to achieve that objective by less infringing means than the pervasive surveillance afforded by Pegasus.
- In many cases, the impact on individual rights and on democratic processes (such as elections) appears to outweigh any security advantage that could have been obtained.
- In some cases, the system appears to have been used in ways that weaken democratic processes, threatening to alter both the formation of public opinion and the outcome of elections.

8.2. The use of spyware in the framework of EU law

In this section, we will make some specific considerations on how the use of spyware can be made consistent with the principles of EU law. We will take into account the fact that, as noted above (Section 7.3), national security activities are exempt from key provisions of data protection law, such as the GDPR and the e-Privacy Directive. If a processing operation counts as a national security activity, then data

subjects are deprived of the protections resulting from such provisions (though they may still refer to other norms of EU law).

Circumscribing the material scope of national security activities

When the concept of national security is used to exclude the application of EU law, its scope needs to be circumscribed, confining its application to threats that genuinely concern the political community as a whole. The need to so delimit this concept stems precisely from its use to limit the scope of EU law, and in particular of data protection instruments. In this context, its interpretation is bound by EU law and has to take into account the intentions of EU legislators, but also the EU constitutional framework.

We have seen that the European Court of Human Rights recognises a wide margin of appreciation for states identifying national security goals and deciding how to go about pursuing them. Indeed, in a recent analysis, the EU Agency for Fundamental Rights found that this concept is relatively undetermined and is understood in different ways in different legal systems.[123]

But the difficulty of determining precisely what falls within national security should not prevent us from clearly identifying what undoubtedly does *not* belong to it. National security cannot include activities designed to (*i*) adversely affect political opponents; (*ii*) influence democratic processes, such as elections, or state functions, such as justice and administration; (*iii*) interfere with the media; (*iv*) target human right activists; (*v*) suppress criticism and dissent; (*vi*) confer special advantages on favoured companies or industries; or (*vii*) benefit or harm members of groups defined by religion, political opinions, ethnicity, race, gender, or other classes of individuals potentially subject to discrimination. If a state adopts measures allegedly aimed at national security, and yet these measures appear to be aimed exclusively or additionally at such unlawful, unfair, or antidemocratic purposes, it should be up to the state to show convincingly that national security grounds exist for these measures, that these measures have no other purpose, and that appropriate precautions to limit any negative side effects have been taken. If evidence to this effect cannot be provided (the state fails to discharge its burden of proof), then we should conclude that such measures fall outside the national security exemption and are subject to full judicial review according to legal standards applicable to the real purpose of such measures.

Circumscribing the personal scope of national security activities

In the previously mentioned judgment in the *Quadrature du Net* case, the ECJ applied the ePrivacy Directive to third parties who were processing (and specifically storing) personal data to comply with an obligation imposed on them for the purpose of national security. Thus, the Court took the view that this third-party processing did not count as a national security activity, even if it was ordered on national security grounds.

To overcome both the ECJ approach and possible suggested extensions of it, the European Council has introduced a new provision in the draft ePrivacy Regulation, stating that the regulation

> *does not apply to the protection of fundamental rights and freedoms related to activities which fall outside the scope of Union law, and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those operations, whether it is a public authority or a private operator acting at the request of a public authority*.

[123] EU Agency for Fundamental Rights. *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU. Volume II: Field perspectives and legal update.* Publications Office of the European Union, 2017.

This amendment should be resisted, since it would give a free hand to states in overriding ePrivacy requirements, and in particular in overriding the prohibition on interfering with users' devices, such as their mobile phones, as set forth in Article 5 of the ePrivacy Directive and reiterated in Article 8 of the proposed ePrivacy Regulation:

> *The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited.*

Including national security activity within the scope of data protection law

Obviously, the approaches just listed only provide a limited opportunity for judicial review. A stronger and less uncertain protection against the abusive use of spyware could be achieved if the provisions excluding the application of the GDPR and the ePrivacy Directive (and Regulation) are revisited, so that national security purposes would only ground restrictions on data protection provisions based on legality and proportionality (rather than a straightforward exclusion from such instruments).

It seems to us that there is a strong case to be made for eliminating such exclusions if surveillance for purposes of national security is to comply with the requirement established by the ECtHR, i.e., legality, necessity, and proportionality, including availability of adequate remedies. As noted, such requirements were also advanced by the ECJ in connection with surveillance in the United States (in the previously mentioned *Schrems I* and *II*). If such a legislative change were undertaken, then in the majority of cases the use of software such as Pegasus would be deemed legally defective under EU law as well.

Supporting the adoption of adequate legal frameworks at the national level

Since national security remains a reserved competence of Member States, it is up to them to effectively ensure that their activity complies with the fundamental rights and principles of EU law. At the same time, however, EU institutions should promote the adoption by Member States of an adequate framework for the use of spyware for national security purposes:[124]

1. **Legality**. Every use of spyware for national security purposes should have its basis in a law that is sufficiently clear and precise to enable individuals to understand under what conditions they may be subject to covert surveillance and for what purposes.
2. **Legitimate end**. The spyware should only be used for a genuine national security purpose, in such a way as to contribute to, rather than detract from, the protection of a democratic society.
3. **Necessity**. The spyware should only be used where the national security goal being pursued cannot otherwise be achieved to the same extent by any less infringing means or in any less infringing way. This entails that information accessed or otherwise retained should be limited to what is relevant to the threat and should be accessed only by authorised bodies and only for the purpose and duration of the authorisation.
4. **Adequacy**. Any use of the spyware should be appropriate to the national security goal being pursued.
5. **Proportionality (balancing)**. The national security benefit to be achieved should outweigh the significance of the interference on individual rights and democratic values. For this purpose, we need to take into account not only the seriousness of abstractly conceivable risk

[124] For some of these requirements, see: Electronic Frontier Foundation and other NGOs (2014). Necessary and Proportionate: On the application of human rights to communication surveillance. https://necessaryandproportionate.org.

scenarios, but also the likelihood that such scenarios will become realities. Thus, for an interference on rights and democracy to be justified, there should be a high probability that a specific threat to national security will be carried out, and also a high probability that the information obtained through the spyware will be useful in identifying or countering such a threat.

6. **Competent authority**. Authorisations and other determinations on the use of the spyware should be provided by an impartial and independent authority having adequate skills and resources.
7. **Due process**. The use of spyware should be subject to review before an independent, competent, and impartial tribunal established by law, with the powers needed to timely enforce the rights of all targeted individuals and provide remedies for any violation.
8. **User notification**. When user devices are hacked, the targeted individuals they belong to should be notified as soon as this can be done without jeopardising the purpose of the surveillance operation.
9. **Transparency**. States should provide adequate publicly accessible information about the legal framework governing the use of spyware (including laws, regulations, activities, powers, or authorities) and about the ways in which spyware is used by state agencies. Moreover, information should be made publicly available about detected misuses of cybersurveillance products.
10. **Public oversight**. States should establish independent oversight mechanisms to ensure transparency and accountability in the use of the spyware. Parliaments should have the ability to carry out effective controls over covert activities by the executive. The oversight bodies through which these controls are carried out should include representatives of the opposition.
11. **Security and certification.** Precise technological requirements should be established for spyware so as to ensure the integrity of the data and the confidentiality of the operations, which should in principle be performed only by competent state officers.
12. **Technical adjustability.** The functionalities of a spyware tool should either be limited to single functions or be customisable, so that, before the spyware is deployed, they can be restricted to what is necessary and lawfully authorised in the case at hand.

8.3. What about Pegasus?

As we have just observed, device-hacking tools may be lawfully deployed by Member States for security or law-enforcement purposes only under appropriate circumstances. Their use should be strictly limited to what is necessary for the legitimate purpose being pursued, be subject to strict and impartial controls and ultimately to judicial review and comply with technical requirements designed to ensure that their operation is secure and effective.

The Commission, as the guardian of the Treaties, should actively engage in investigating the use of spyware and assuring that the EU law is respected, and its values implemented. The EU Parliament has a fundamental role to play in this regard, not only through its participation in the enactment of relevant legislative instruments (such as the proposed ePrivacy Regulation), but also through its investigative activities and its interactions with national parliaments and governments, the media, and the public.

The PEGA Committee has indeed been very effective in collecting and processing evidence on the use of Pegasus, and in providing extensive publicly accessible information and critical perspectives.[125] The activity of the Committee has indeed shown the importance of recognising to the Parliament broad investigatory powers, as a necessary complement to its legislative and political responsibilities.[126]

Different initiatives should be taken relative to the use of device-hacking tools:

- Consistently applying existing national and EU law (including the Treaties, the Charter, and the European Convention on Human Rights) to assess the lawfulness of existing practices.
- Urging states that deploy spyware tools to equip themselves with adequate, organisational, technological, and legal frameworks, in the absence of which any use of device-hacking software would be unlawful and should therefore be stopped.
- Engaging experts and civil society in a political, ethical, and technological debate on the use of device-hacking systems, their impacts, and the alternatives.

As previously noted, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression proposed a moratorium on the use of spyware.[127] This is a view we may in principle subscribe to: according to a proportionality assessment responsive to empirical situations, the very existence of widespread abuses in the deployment of a device-hacking system could justify the suspension of their use until all technological, legal, or organisational issues that have enabled such abuses have been satisfactorily addressed. A global, albeit provisional, ban on device-hacking would undoubtedly be the most effective way to prevent the widespread abuses we have witnessed.

However, in standing behind the idea of a general moratorium on the use of device-hacking spyware —understood as a global ban on its use, until measures can be developed preventing abuse globally— we have to deal with the fact that most states in the world, including all EU Member States, are currently using spyware tools. Device-hacking is explicitly recognised in certain national legislations, such as the Italian one,[128] and many in law enforcement and the security forces regard it as an important part of their toolbox, a judgement that is shared by many politicians.

Thus, rather than recommending that all Member States immediately and unconditionally relinquish all device-hacking tools, we would see it as politically more feasible if a moratorium on the use of these tools is made to consist in a strong presumption against the lawfulness of their use. This presumption is grounded in the extensive evidence of their abusive deployment in many countries, and should only be overcome when a state convincingly shows a willingness and a capacity to prevent all abuses by consistently and effectively implementing all measures required (see Sections 8.1 and 8.2) to ensure consistency with fundamental rights, democracy, and the rule of law.

Moreover, all Member States should be urged to ban the use of specific spyware tools where there is strong evidence that such tools have already been used for unlawful activities, especially within the EU. In the case of Pegasus, we may ask whether such abuses are to be attributed to the very nature of Pegasus —to its technical features, such as its general scope, which makes for maximal intrusiveness,

[125] https://www.europarl.europa.eu/committees/en/pega/home/highlights.

[126] A parallel with the U.S. could be useful where the Supreme Court has long since accorded its agreement with Congress that the investigatory power is so essential to the legislative function as to be implied from the general vesting of legislative power in Congress. See McGrain v. Daugherty, 273 U.S. 174 (1927): " the power of inquiry —with process to enforce it— is an essential and appropriate auxiliary to the legislative function."

[127] United Nations. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2014; Kaye, David. The impact of spyware on fundamental rights.

[128] Legislative decree 29 December 2017, n. 216, as modified by the law 28 February 2020, n 7.

and the absence of adequate guarantees about the security and integrity of the data it collects and transmits— or whether the abuses are rather owed to the commercial, institutional, organisational, and political frameworks in which this technology has been deployed. Either way, the very extent of these abuses justifies a ban on the use of Pegasus (including its purchase, sale, import, and export). Until there is clear evidence that such unacceptable practices no longer take place, continuing to deploy Pegasus, even in the framework of lawful activities, amounts to supporting its production and distribution, and thus involves a political (even if not a legal) complicity in such practices.

REFERENCES

- Amnesty International. *Forensic Methodology Report. How to Catch NSO Group's Pegasus*. 2021.
- *Lessons from the Stasi – A cautionary tale on mass surveillance*. 2015, url: https://www.amnesty.org/en/latest/news/2015/03/lessons-from-the-stasi/.
- Arendt, H. "The Crisis in Education." In *Between Past and Future - Six Exercises in Political Thought*. Viking, 1961 [1954].
- Auriel, P., Beaud, O., and Wellman, C. *The Rule of Crisis Terrorism, Emergency Legislation and the Rule of Law*. Springer, 2018.
- Beckman, L. "Democracy." In *Oxford Research Encyclopedias, Politics*. Oxford University Press, 2021.
- Benjakob, O. "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer Is Building a New Empire", *Haaretz* (2022 - 20 September).
- Boffey, D. "EU Commissioner calls for urgent action against Pegasus spyware." *The Guardian* (2021 - 15 September).
- Buchta, A. and Kranenborg, H. Institutional report topic 2: The new EU data protection regime. In The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection. TheXXIX FIDE Congress in the Hague. Eleven, 2020, pp. 79–105.
- Christiano, T. and Sameer B. "Democracy." In *The Stanford Encyclopedia of Philosophy*. Stanford University, 2022.
- Clarke, R. A. et al. *The NSA Report, Liberty and Security in a Changing World*. Princeton University Press, 2014.
- Commission of the European Communities. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*. COM (2020) 790 final, 2020.
- Council of Europe. *Mass surveillance: Who is watching the watchers?* Council of Europe Publishing, 2016.
- De Witte, B. "Exclusive Member State Competences – Is There Such a Thing?" In *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*. Hart, 2017, pp. 59–73.
- EDPS. *Preliminary Remarks on Modern Spyware*, 2022. https://edps.europa.eu/system/files/2022-02/22-02-15edpspreliminaryremarksonmodernspywareen0.pdf
- Electronic Frontier Foundation and other NGOs. *Necessary and Proportionate: On the application of human rights to communication surveillance*. 2014, url https://necessaryandproportionate.org/principles/.
- EU Agency for Fundamental Rights. *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU. Volume II: Field perspectives and legal update*. Publications Office of the European Union, 2017.
- European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling online disinformation: a European approach*. COM (2018) 236 final, 2018.

- European Council. *Internal security strategy for the European Union Towards a European security model.* Publications Office of the European Union, 2010.
- European Court of Human Rights. *Guide to the Case-Law of the European Court of Human Rights. Data protection.* Council of Europe Publishing, 2022.
- European Parliament. *Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*. 2013/2188(INI), P7-TA (2014)0230, 2014.
- European Parliament. Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware Rapporteur: Sophie in 't Veld (2022). *Draft Report*.
- General Secretariat of the Council. *European Security Strategy. A Secure Europe in a Better World*. 2009.
- Gutheil, M., Liger, Q., Heetman, A., Eager, J., and Crawford, M. *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices.* Study requested by the LIBE committee. European Parliament, 2017.
- Habermas, J. *Legitimation crisis*. Beacon Press, 1975.
  - "Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research." In *Communication Theory* (2006), pp. 411–426.
- Human Rights Committee. *General comment No.34 on Article 19: Freedoms of opinion and expression.* United Nations. CCPR/C/GC/34, 2011.
- Kathrine, G.J.W., Praise, P.M., Rose, A.A. and Kalaivani, E.C., 2019. "Variants of phishing attacks and their detection techniques." In *3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2019, pp. 255-259
- Kaye, D. *The impact of spyware on fundamental rights.* Testimony to the PEGA Committee of the European Parliament, 27 October 2022.
- Legrand, T. National Security and Public Policy: Exceptionalism Versus Accountability. In *The Palgrave Handbook of National Security*. Ed. by Michael Clarke et al. 2022. Chap. 3.
- Litwiński, P. *Opinia prawna w sprawie naruszeń, w związku z ujawnionymi przypadkami użycia oprogramowania szpiegującego Pegasus w świetle prawa ochrony danych osobowych, przepisów Karty Praw Podstawowych UE i Konstytucji RP*, Kancelaria Senatu, Warszawa 2022
- Liu, W. and Zhong, S. "Web malware spread modelling and optimal control strategies." *Scientific reports*, 7(1), 2017. pp.1-19.
- Lyon, D. *Surveillance Studies*. Polity Press, 2007.
- Mansbridge, J et al. "A systemic approach to deliberative democracy." In *Deliberative Systems: Deliberative Democracy at the Large Scale*. Ed. by John Parkinson and Jane Mansbridge. Cambridge University Press, 2012, pp. 1–26.
- Marx, G. T. *Windows into the Soul. Surveillance and Society in an Age of High Technology.* Chicago University Press, 2016.
- Marzocchi, O. and Mazzini, M. *Pegasus and surveillance spyware.* European Parliament. PEGA Committee, 2022.

- Mazetti, M., Bergman, R., and Sevis-Grindneff, M. "US strains to control spyware, but uses it." *The New York Times.* (1 December 2022).
- Newman, Lily Hay. "Google Warns That NSO Hacking Is On Par With Elite Nation-State Spies." *Wired* (15 December 2021).
- Monti, A. and Wacks, R. *National Security in the New World Order.* Routledge, 2022.
- Nisha, T.N. and Kulkarni, M.S., "Zero click attacks–a new cyber threat for the e-banking sector." *Journal of Financial Crime*, (ahead-of-print), 2022.
- NSO. *Pegasus - Product Description.*
- Rankin, J. "Dutch MEP says illegal spyware 'a grave threat to democracy." *The Guardian* (8 November 2022).
- Rijpma, J. J. "The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection." *The XXIX FIDE Congress in the Hague*. Eleven, 2020.
- Rodotà, S. "Data Protection as a Fundamental Right." In *Reinventing Data Protection?* Ed. by Serge Gutwirth et al. Springer, 2009, pp. 77–82.
- Saeed, I.A., Selamat, A. and Abuagoub, A.M., "A survey on malware and malware detection systems." *International Journal of Computer Applications* (2013), 67(16).
- Sahani, R. and Randhawa, S., "Clickjacking: Beware of Clicking." *Wireless Personal Communications* (2021) 121(4), pp.2845-2855.
- Salahdine, F. and Kaabouch, N., Social engineering attacks: A survey. *Future Internet* (2019), 11(4), p. 89.
- Sanders, B. "Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections." In: Chinese Journal of International Law (2019), pp. 1–56.
- Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. and Ng, A. Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data* (2020) 7(1), pp.1-29.
- Schmitt, C. *Political Theology*. MIT, 1985 [1922].
- Simitis, S. "Reviewing Privacy in the Information Age." In *University of Pennsylvania Law Review* (1987), pp. 707–46.
- Singh, U.K., Joshi, C. and Kanellopoulos, D., 2019. A framework for zero-day vulnerabilities detection and prioritization. Journal of Information Security and Applications, 46, pp.164-172.
- United Nations. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/23/40, 2013.
- United Nations, General Assembly. *The right to privacy in the digital age: resolution.* United Nations. A/RES/73/179, 2019.
- United Nations. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye.* A/HRC/41/35, 2019.

  - Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders. A/HRC/40/52, 2019.

  - Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. A/HRC/34/60, 2017.

- Vogiatzoglou, P., Marquenie, T., and Valke. P. *Assessment of the implementation of the Law Enforcement Directive. Study requested by the LIBE committee.* European Parliament, 2022.
- Watt, E. *State Sponsored Cyber Surveillance.* Elgar, 2021.

This study - commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA) - analyses the impact of the use of Pegasus and similar spyware has on Article 2 TEU values, on privacy and data protection, and on democratic processes in Member States.

PE 740.514
IP/C/PEGA/IC/2022-071

Print ISBN 978-92-848-0096-4 | doi: 10.2861/981463 | QA-03-22-291-EN-C
PDF ISBN 978-92-848-0097-1 | doi: 10.2861/031930 | QA-03-22-291-EN-N