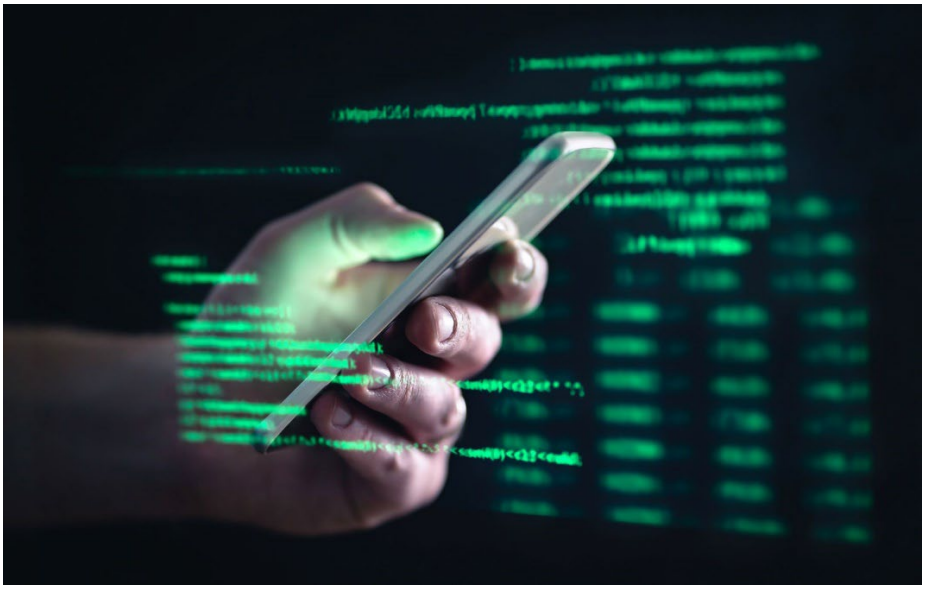
STUDY

Requested by the PEGA committee

European Parliament

The use of Pegasus and equivalent surveillance spyware

The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware



Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 740.151 – February 2023

EN

The use of Pegasus and equivalent surveillance spyware

The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware

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), provides a description of the legal framework (including oversight and redress mechanisms) governing the use of Pegasus and equivalent spyware in a selection of Member States.

This document was requested by the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware.

AUTHORS
Quentin LIGER, Asterisk Research and Analysis GmbH
Mirja GUTHEIL, Asterisk Research and Analysis GmbH

ADMINISTRATOR RESPONSIBLE
Ottavio MARZOCCHI

EDITORIAL ASSISTANT
Sybille PECSTEEN de BUYTSWERVE

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: poldep-citizens@europarl.europa.eu

Manuscript completed in February 2023

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

DISCLAIMER AND COPYRIGHT

CONTENTS

LIST OF ABBREVIATIONS

ADAE	Authority for Communication Security and Privacy (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών) - Greece
AISE	External Information and Security Agency (Agenzia Informazioni e Sicurezza Esterna) – Italy
AISI	Internal Information and Security Agency (Agenzia Informazioni e Sicurezza Interna) - Italy
AIVD	General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst) – the Netherlands
BGHSt	Federal Court of Justice in Criminal Cases (*Entscheidungen des Bundesgerichtshofes in Strafsachen) – Germany*
BKA	German Federal Criminal Police Office (Bundeskriminalamt) - Germany
BND	Federal Intelligence Service (*Bundesnachrichtendienst)* -Germany
Cibdu	Inter-ministerial Commission of Dual-Use Goods (*commission interministérielle des biens à double usage*) – France
CNCTR	Commission for Oversight of Intelligence Gathering Techniques (*Commission nationale de contrôle des techniques de renseignement*.) - France
CNI	National Intelligence Service (*Centro Nacional de Inteligencia*) - Spain
CNIL	National Commission on Informatics and Liberty *(Commission Nationale de l'Informatique et des Libertés)* - France
COPASIR	Parliamentary Committee for the Security of the Republic (*Comitato parlamentare per la sicurezza della Repubblica)* - Italy
DDD	Defender of Rights (*Défenseur des Droits*) - France
DGSE	Directorate General of External Security (*Direction générale de la sécurité extérieure* - France
DGSI	Directorate General of Interior Security (*Direction générale de la sécurité intérieure)* - France
DNRED	National Directorate of the Intelligence and Customs Investigations (Direction Nationale du Renseignement et des Enquêtes Douanières - France
DRSD	Directorate of Intelligence and Security of Defence (Direction du Renseignement et de la Sécurité de la Défense - France
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EUR	Euro

EYP	National Intelligence Service (*Ethnikí Ypiresía Pliroforión*) - Greece
GDPR	General Data Protection Regulation
HCLU	Hungarian Civil Liberties Union
HDPA	Hellenic Data Protection Authority
HPiD	Hellenic Police Intelligence Division (*Διεύθυνσης Διαχείρισης και Ανάλυσης Πληροφοριών) Greece*
ICCPR	International Covenant on Civil and Political Rights
MIVD	Dutch Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdiens) – the Netherlands
NAIH	Hungarian National Authority for Data Protection and Freedom of Information
NBSZ	Special Service for National Security (Nemzetbiztonsági Szakszolgálat) - Hungary
NIK	Supreme Audit Office - Poland
PEGA	Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware
PiS	Law and Justice (*Prawo i Sprawiedliwość*) – Poland
PLN	Polish złoty
PO	Civic Platform (*Platforma Obywatelska)* - Poland
StGB	*German Criminal Code* (Strafgesetzbuch)
StPO	Code of Criminal Procedure (*Strafprozessordnung*) – Germany
Wiv	Intelligence and Security Services Act (Wet op de inlichtingen- en veiligheidsdiensten) - Netherlands
ZITiS	Office for Information Technology in the Security Sector (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich*) - Germany

EXECUTIVE SUMMARY

In 2017, the European Parliament commissioned a study on "**Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices**"[1]. The study examined the legal frameworks and practices for hacking by law enforcement drawing upon the international and EU-level debates on the topic. The study came on the back of high-profile cases where law enforcement authorities were unable to gain access to material needed for specific investigations. It looked into the risks that the use of hacking techniques present to the security of the internet as well as to privacy and fundamental rights. It focused on tools developed by law enforcement authorities and examined commercial hacking and spyware products only tangentially.

Fundamental Rights, such as the right to privacy, to data protection and to the freedom of expression, **are cornerstones of the European legal order**. Restrictions on these rights are possible under the Charter of Fundamental Rights of the EU provided that they are proportionate and necessary. These restrictions exist to allow law enforcement and intelligence agencies to fight crime and protect national security. The Codes of Criminal Procedure of all Member States, assessed as part of this study, provide for the use of special investigative techniques which may include, explicitly or not, hacking and the use of spyware. When investigating certain crimes, these limitations allow the police to use these techniques following due process and judicial authorisation for specific periods of times. Intelligence services also use similar techniques, including spyware. The framework within which these operate is more opaque, in part due to the secretive nature of their operations. **The existence of robust ex-ante and ex-post oversight mechanisms is therefore crucial** to ensure intelligence services operate according to standards acceptable to democratic societies, as set out by the Venice Commission.

In July 2021, CitizenLab, Amnesty International, Forbidden Stories and 17 media organisations[2] broke the news that Pegasus and equivalent spyware was used on a large scale by governments (including European ones) to target people, including activists, opposition figures, journalists, diplomats, and members of the judiciary. This led to questions in different Member States and beyond as to who was responsible for the use of Pegasus and equivalent spyware. To date, NSO, the company that created Pegasus, has admitted having sold the software to 14 EU Member States. Other equivalent spyware used by EU governments has also been identified by companies, civil society organisations and investigative journalists, including Predator and Candiru.

In all the countries covered by this study, **there is a legal framework for the use, import, sale,** etc. of cyberweapons, including Pegasus or equivalent spyware. In all cases, however, **this framework**, which applies to the general population, **includes specific exceptions for law enforcement and intelligence agencies**. Their use is often included under the umbrella of "special investigative techniques", and is regulated by criminal procedural codes, laws on internal security or equivalent measures.

In democratic societies, a **balance** has to be reached in ensuring that intelligence and security services can operate effectively, while complying with democratic norms and standards. Public accountability is necessary to minimise abuses of power. In a number of countries covered in this report, there has been a lack of accountability in the acquisition and use of Pegasus and equivalent spyware.

[1] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

[2] See Forbidden Stories website, available at: https://forbiddenstories.org/case/the-pegasus-project/

More specifically, there is a **high level of opacity around the process involved in purchasing** Pegasus or equivalent spyware. This partly stems from the complex structure of companies such as NSO, which operate through different legal entities located within and outside of the EU. The way in which the spyware is procured is also difficult to trace. In some cases, such as **Germany**, the Central Office for Information Technology in the Security Sector (ZITiS) was not involved in the procurement of the software by the German Federal Criminal Police Office (BKA). In other cases, such as **Greece**, investigative journalists claim that the Predator spyware has been used by the intelligence service, while the State claims it did not purchase the software.

Oversight mechanisms on the use of special investigative techniques - notably those involving spyware such as Pegasus or similar - should operate to guarantee the full respect of the law and fundamental rights, but appear to be **very weak or completely inefficient in some Member States**. A **lack of independence of the oversight mechanisms in Hungary, Greece, Poland and Spain** has led to what can only be described as **abusive use of Pegasus of equivalent spyware**. The **Netherlands**' system of having a committee made of two magistrates and one technical expert providing a binding decision on the use of special investigative techniques appears to be a robust solution, albeit one that is open to criticism.

The glaring gap identified in this report is the **ineffectiveness of redress mechanisms** when a decision to use Pegasus or similar spyware has been taken. Instances of abuse of these spywares have been identified by investigative journalists, civil society or private organisations. Effective ex-post oversight mechanisms should have uncovered controversial instances of the use of Pegasus and equivalent spyware by law enforcement and intelligence agencies against domestic journalists, politicians and civil rights activists. These should have included also appropriate and effective individual and collective redress mechanisms to bring justice and ensure such abuses will not take place in the future.

The capabilities of Pegasus and equivalent spyware, allowing access to a devices' content, its metadata, and the possibility to remotely record video and audio inputs are **extremely invasive**. According to the European Data Protection supervisor (EDPS), it is 'unlikely to meet the requirements for proportionality' set out by the CJEU and the ECtHR. In addition to the fundamental rights aspects of surveillance, there are concerns about involving **private companies** in intrusive investigation procedures, while fundamental rights primarily bind the state and not necessarily spyware providers.

The 2017 study identified how law enforcement authorities had experienced an exponential increase in the data they could access through gaining control of a device, including data which may not have been relevant to the initial investigation. This risk is again exacerbated by technologies such as Pegasus and equivalent spyware, given how intrusive they are. Since the fundamental rights risks of using such tools are unlikely to meet the proportionality test, the regular deployment of Pegasus or similar spyware would not be compatible with the EU legal order.

Consequently, some of the **recommendations** of the 2017 report remain valid and have been updated. They relate to the need of more research on the effectiveness of **oversight mechanisms** and the need for Member States to **adopt clear and effective legal frameworks**.

It is further recommended that Member States **refrain from using technologies** that have a clear disproportionate impact on human rights, and that their **proportionality, effectiveness and use** should be monitored.

Clearer and stronger regulation of the market for Pegasus or equivalent spyware is recommended. The European Parliament could request the Commission to submit a legislative proposal to require that

all **surveillance companies** domiciled in their countries act responsibly and are held liable for the negative human rights impact of their products and services.

Given the importance of civil society organisations and investigative journalists in uncovering the abuse of Pegasus and equivalent spyware, the final recommendation is for the European Parliament to continue its efforts to support the **freedom and independence of the press**, as well as its efforts to protect **whistle-blowers**.

1. INTRODUCTION

1.1. Overview

This report builds on a study published in 2017 on "**Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices**"[3]. The study examined the legal frameworks and practices for hacking by law enforcement by analysing the international and EU-level debates on the topic. The term "hacking" was used in the study as a technique to bypass encryption and carry out surveillance and/or gathering evidence by law enforcement authorities. The present study provides an update on the 2017 one, extending its scope to **focus on Pegasus and equivalent surveillance spyware**. It also extend its scope by describing the use of such tools by a wider range of actors, including intelligence agencies.

This report provides an update on to Member States covered by the 2017 study, namely **France, Germany, Italy, the Netherlands and Poland** as well as information on **Hungary, Spain and Greece**.

The study focusses on the **acquisition and use** of surveillance spyware such as Pegasus. The objectives of the project are as follow:

- **Objective 1** - describe the existing legal framework in selected EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware, in relation to law enforcement agencies, intelligence services, the police, the military, companies and private parties;
- **Objective 2** - describe the regimes for ex ante and ex post judicial and democratic oversight; and redress mechanisms in case of illegal use by the abovementioned actors;
- **Objective 3** - describe the ECHR and EU law and jurisprudence requirements in terms of compatibility with international standards;
- **Objective 4** - make recommendations to the EU and its institutions, to Member States, to stakeholders, on the above issues based on the best practices identified.

1.2. Structure of the final report

This report is structured as follows:

Executive summary

- **1. Introduction** – this section sets out the scope of the study and its objectives;
- **2. General Framework** – setting out the context for this study as well as key definitions;
- **3. The use of Pegasus and similar spyware** provides an overview of the use of Pegasus and similar spyware in the focus countries;
- **4. Legal framework for acquisition and use** provides an overview of the legal frameworks on the acquisition and use of Pegasus and other similar software including sanctions and penalties;
- **5. Oversight and redress** describes the ex-ante and ex-post oversight and redress mechanisms in place in the focus countries;

[3] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

- **6. Fundamental Rights considerations** provides a discussion of international fundamental rights standards, including a summary of relevant CJEU and ECtHR case law as well as standards set out by the Venice Commission;
- **7. Conclusions and recommendations.**

2. GENERAL FRAMEWORK

The **right to privacy** and having one's personal data protected from interference is a cornerstone of the European legal order[4]. **Limitations to these rights exist**, particularly in order to allow **Law Enforcement Agencies** and other state actors, including **intelligence services** to collect information and evidence in criminal investigations and cases where there is a threat to national security through **special investigative techniques**. Historically, the limits to the right to privacy were undertaken using coercive measures which were limited in scope and in their invasiveness (through house searches, wiretapping etc.). The increased reliance on connected devices, in particular mobile telephones and computers, increases the amount of information which can be collected. **Hacking a device allows for access to all data held on a device, as well as all information flows in and out of the device**; this is likely to constitute the collection of a much greater amount of data, as well as the collection of much more sensitive data. Special investigative techniques include the hacking of devices and gaining access to them through hacking and the use of spyware. Law enforcement representatives, state that the use of hacking techniques as an investigative tool brings significant improvements in investigative effectiveness.[5] Although the use of hacking techniques will bring improvements in investigative effectiveness, the significant amount and sensitivity of data that can be accessed through these means acts as a stimulus for another key debate: **ensuring the protection of the fundamental right to privacy**.

In **criminal investigation** cases, the police or the public prosecutor are generally in charge of requesting the use of special investigation techniques. A judge or a court are responsible for authorising and monitoring the procedure. Table 1 below summarises the procedure of the use of special investigative techniques in the countries covered by this study.

Table 1: Authorisation of special investigative techniques in criminal law

	EL	ES	HU	PL	DE	FR	IT	NL
Who can request	Investigative authority	PP	PP	Investigative authority	PP or Federal Criminal Police Office	PP or investigative judge	PP	PP
Who authorises?	Prosecutor or judicial council	Judge	Judge	Judge (local district court)	Judge (court)	Judge	Judge	Investigative judge

* PP: Public Prosecutor

Intelligence services are governed by different procedures, reflecting the framework in which they operate, which may require speed and more secrecy. As such, the request and authorisations procedure are different. Due to the secrecy of some of the intelligence services actions, the rules governing their operations can often be secret. **Oversight mechanisms**, both in the time leading to

[4] As reflected in the European Convention on Human Rights and the Charter of Fundamental Rights of the EU. See Chapter 6 for a review of the legal framework.

[5] IACP Summit Report. 2015. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence.

the use of special investigative techniques (ex-ante) or after they have been completed (ex-post) mechanisms **are therefore necessary**. These oversight mechanisms help ensure intelligence agencies operate within the law, while being able to do so with an adequate amount of secrecy. These mechanisms include internal control procedures, parliamentary oversight, judicial review and redress in cases where the law has been broken.

This study examines the existing framework in eight Member States, in order to assess whether there are similarities, and practices that can be identified. The **emergence of the Pegasus** scandal has provided a real-life test of the effectiveness and efficiency of these mechanisms.

The box below provides the definition of key terminology

Box 1: Terms and definitions used in this report

Hacking - a situation in which someone abuses their authority to illegally access an information network while using a computer or another information processing device.

Intelligence service - a government department involved in the gathering of military or political information, especially in the interests of national security.

Law Enforcement Authorities – a government agency responsible for the enforcement of the laws (police, gendarmerie or equivalent).

Special investigative measures or techniques are a way for gathering information systematically in such a way as not to allow the target person to know of them[6].

Spyware - software that is installed on a user's computer without their knowledge. Such software transmits information on the user and his habits once connected to the internet.[7]

Surveillance – monitoring of behaviour, activities, or information for the purpose of information gathering, influencing, managing or directing.[8]

Tapping - connecting a listening device to a telephone line to monitor conversations secretly.

[6] See Eurojust, https://www.eurojust.europa.eu/judicial-cooperation/instruments/special-investigative-measures

[7] European Commission definition in Communication from the Commission of 15 November 2006 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software [COM(2006) 688 final -

[8] Lyon, David (2001). Surveillance Society: Monitoring in Everyday Life. Philadelphia: Open University Press.

3. THE USE OF PEGASUS AND SIMILAR SPYWARE

The widespread use of Pegasus and equivalent spyware was revealed thanks to the combined work of Citizen Lab, Amnesty International, Forbidden Stories and 17 media organisations.[9] Citizen Lab had been aware of the existence of the spyware since 2015 and had reported on it since 2016. The revelations in July 2021 that the spyware had been used by governments (including European ones) to target people including activists, opposition figures, journalists, diplomats, and members of the judiciary, led to a public debates as to who was responsible for the use of Pegasus and equivalent spyware. To date NSO, the company having created Pegasus, has admitted having sold the software to 14 EU Member States.

Since the story broke, new information has emerged on the use of Pegasus or equivalent spyware by governments across the world and specifically in the EU. In April 2022, the use of Pegasus, Candiru and equivalent spyware was confirmed to have been used by the **Spanish** intelligence service to target *inter alia* politicians and civil society members. In August of the same year, the focus shifted to **Greece**, where journalists and politicians' phones were found to have been hacked by the Predator spyware.

Spyware is not new, even though the **capabilities** of spyware such as Pegasus, Predator and Candiru **exceed what existed in the past**. The use of hacking tools by law enforcement and intelligence services has been widely discussed since the release of detailed information on Gamma Group's spyware suite, *FinFisher*,[10] and the practices of Italian firm *Hacking Team*,[11] in 2012. These are discussed in greater detail in the report on hacking by law enforcement authorities published in 2017.[12]

In this chapter, a brief overview of the use of Pegasus or equivalent spyware in the focus countries is provided. Countries where the use of these spyware has either been confirmed or strongly suspected are presented first.

Countries in this and subsequent chapters are presented in the following order: first, countries where the use of Pegasus and equivalent spyware has been used in ways deemed problematic (EL, ES, HU, PL); second, the remaining Member States examined in this study (DE, FR, IT, NL). For each group, countries are listed in the protocol order in which countries based on the alphabetical list of countries in their national language.

3.1. Greece

Greece is one of the countries where Pegasus and other similar spyware has been used by government agencies to target its own citizens.

Greece has experienced the fallback from the use of the **Predator** spyware to monitor journalist and opposition politicians. In November 2021, *Efimerida ton Syntakton* published a story showing that a journalist was the subject of surveillance by the National Intelligence Service (Ethnikí Ypiresía

[9] See Forbidden Stories website, available at: https://forbiddenstories.org/case/the-pegasus-project/

[10] Marczak, B. et al. 2015. Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. Munk School of Global Affairs.

[11] Reporters without Borders. 2012. The Enemies of Internet, Special Edition: Surveillance. Available at: http://surveillance.rsf.org/en/hacking-team/.

[12] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.

Pliroforión - EYP).[13] **Stavros Malichudis**, an investigative journalist reporting on migration issues recognised himself as the target of the surveillance. This was followed by CitizenLab revelation that investigative journalist **Thanasis Koukakis'** phone had been hacked by the Predator spyware. Since then, other journalists and politicians' phones were found to have been hacked by the same spyware. In July 2022. **Nikos Androulakis**, MEP and president of the PASOK-KINAL opposition movement, announced that he was filing a lawsuit as he had been targeted with an attempt to hack his phone in September 2021.[14]

These allegations led to the **resignation** of the Director of the EYP, as well as of Grigoris Dimitriadis, the Secretary General of Prime Minister Kyriakos Mitsotakis, whose role was to oversee the Service.[15]

In the works of CitizenLab, which identified the spyware's use in Greece, "***Predator*** *is a surveillance tool that offers its operator full and continuous access to the target's mobile [phone] device. Predator allows the operator to extract secret passwords, files, photos, web browsing history, contacts as well as data such as mobile device information […] take screen captures, record the user's entries,[…] activate the device's microphone and camera, […] record text messages sent or received[…] as well as normal and VoIP phone calls*".

The main difference with Pegasus is that Predator is a one-click exploit and therefore requires the target to click on a link in order for the spyware to infect their phone. Predator is marketed openly in the country. When first discovered, it was reported to be marketed by Cytrox, a firm based in North Macedonia. It has since been established that the firm is part of the wider Israeli companies' network **Intellexa**. The name refers to "*a brand name for a collection of different firms offering cyberoffense technologies and services, from spyware to open-source intelligence*"[16].

More recently, media revealed that more than 50 people had been spied upon, while ADAE reportedly confirmed that a cabinet minister and senior figures in the armed forces had also been placed under surveillance.[17]

3.2. Spain

Spain is one of the countries where Pegasus and other similar spyware has been used by government agencies to target its own citizen.

[13] Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ, November 2021, available at: https://www.efsyn.gr/themata/thema-tis-efsyn/319063_polites-se-kathestos-parakoloythisis-apo-tin-eyp

[14] Kathimerini, PASOK chief files complaint over alleged phone tap attempt, August 2022, available at: https://www.ekathimerini.com/news/1189916/pasok-chief-files-complaint-over-alleged-phone-tap-attempt/

[15] Kathimerini, Wiretapping case triggers political unrest, August 2022, available at: https://www.ekathimerini.com/news/1190674/wiretapping-case-triggers-political-unrest/

[16] Haaretz, As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer Is Building a New Empire, 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

[17] The Guardian, Greek government faces confidence vote over spying row, January 2023, available at: https://www.theguardian.com/world/2023/jan/25/opposition-file-no-confidence-motion-greek-watergate-scandal-prime-minister-kyriakos-mitsotakis-wiretaps

In July 2020, a joint investigation by El País and the Guardian revealed that Roger Torrent, the speaker of the Catalan parliament and at least two other pro-independence leaders were targeted by spyware in the 2019.[18]

In April 2022, Citizen Lab broke the story that at least 65 individuals had been targeted or infected by mercenary spyware. While the in the majority of cases the spyware used was Pegasus, in some cases Candiru was also used. The victims were mainly individuals active in the pro-independence movement in Catalonia. Victims include Members of the European Parliament, Catalan Presidents, legislators, jurists and members of civil society organisations.[19] Citizen Lab did not attribute the attacks to a specific entity, but suggested that circumstantial evidence pointed to a "*strong nexus with one or more entities within the Spanish government*".[20] Citizen Lab lists four points in particular: (i) the targets were of obvious interest to the government, (ii) the timing of the targeting matches moments and events of specific interest to the government, (iii) the baits used to target the victims suggests the attackers had access to the victims' personal information (including governmental ID number), and (iv) the National Intelligence Centre (CNI) had reported being a customer of the NSO group and the Ministry of Interior is reported to possess similar capabilities.[21] The CNI has been suspected of having acquired or used spyware in the past, including FinFisher, as well as other types of spyware.

Shortly after, the Spanish government organised a press conference to announce that the phones of the Prime Minister and the Minister of Defence Margarita Robles (heading the two organisations overseeing the CNI) has been targeted by the Pegasus spyware.[22] While no confirmation of the source of these attacks have been given, there are strong suspicions that the Moroccan authorities (which are suspected to have used Pegasus against targets in France and Italy – see the respective sections on these countries) are responsible for such surveillance operations, in relation to the ongoing discussions about the fate of Western Sahara.[23] The timing of the revelations was seen by some opposition politicians as a smoke screen to hide CNI's role in the scandals uncovered by CitizenLab. This also represented a unique case of a government disclosing information on surveillance operations that had not been revealed beforehand by investigative journalists, NGOs or companies.

In a closed-door meeting of the Spanish parliament's "Commission for the Control of Credits Allocated to Reserved Expenditures" (commonly referred to as the officials' secret commission), the CNI admitted to being responsible for the targeting of 18 pro-independence activists - but claimed it had done so

[18] The Guardian, Phone of top Catalan politician 'targeted by government-grade spyware', July 2020, available at: https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware

[19] Citizen Lab, CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru, April 2022, available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

[20] Ibid.

[21] Ibid.

[22] Mediapart, Pegasus : Pedro Sánchez espionné, la confusion politique gagne l'Espagne, May 2022, available at: https://www.mediapart.fr/journal/international/020522/pegasus-pedro-sanchez-espionne-la-confusion-politique-gagne-l-espagne

[23] NPR, A spying scandal and the fate of Western Sahara, May 2022, available at: https://www.npr.org/2022/05/11/1098368201/a-spying-scandal-and-the-fate-of-western-sahara

under authorisation from the Supreme Court.[24] There is a discrepancy between what was admitted in the Commission and the 63 people targeted according to CitizenLab.[25]

A few days later, Paz Esteban, the Director of the CNI, was replaced after calls by some politicians and civil society organizations to restore confidence in the country's intelligence community.

No parliamentary inquiry committee has been set up to look into the case.

3.3. Hungary

Over 300 people are suspected to have been the **target of the Pegasus spyware** in Hungary. An investigation by Direkt36, one of the Pegasus Project's media partners showed the journalists, lawyers, businesspeople as well as politicians had potentially been targeted by the spyware.[26] The news, which broke in July 2021, was initially followed by a period during which the government neither commented nor denied the use of Pegasus. In November 2021, Lajos Kosa, chair of the Parliament's Defence and Law Enforcement Committee, told reporters that **Hungary has indeed purchased Pegasus** but that it only had been used with all the legal considerations (i.e. with permission from a judge or the Minister of Justice).[27]

In 2017, the Hungarian parliament's national security committee voted on the possibility for the country's intelligence services to acquire certain equipment with following the normal public procurement procedure. At the request of the Special Service for National Security (Nemzetbiztonsági Szakszolgálat, NBSZ), parliament supported the **acquisition** of a sophisticated spyware which turned out to be NSO's Pegasus.[28]

The acquisition of the spyware appears to have been complex. Rather than the Hungarian State and NSO drawing a direct contract, **a Hungarian intermediary company bought the spyware from a company with links to NSO, registered in Luxembourg**. The purchase is reported to have costed approximately 6 million Euros. The intermediary company, Communication Technologies Ltd. Is partly owned by Péter Neuman, a former intelligence officer with links to politicians, as well as László Hetényi, who had served as a security officer in the Interior Ministry. The company's third owner, László Tasnádi, is a former state secretary at the Interior Ministry and reported to be a close friend of the current Minister of Interior, Sándor Pintér.[29]

[24] El Nacional, Spain's CNI admits spying on Aragonès and on Puigdemont's circle, with court approval https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html

[25] CitizenLab, CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru, available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

[26] Direkt36, Hungarian journalists and critics of Orbán were targeted with Pegasus, a powerful Israeli cyberweapon, available at: https://www.direkt36.hu/en/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele https://telex.hu/direkt36/2021/07/23/az-orban-kormany-allamtitkarat-is-megceloztak-a-pegasusszal-mikozben-belharcokat-vivott-paks-ii-miatt

[27] The Record, Hungarian official confirms government bought and used Pegasus spyware, November 2021, available at: https://therecord.media/hungarian-official-confirms-governments-bought-and-used-pegasus-spyware/

[28] Direkt36, The inside story of how Pegasus was brought to Hungary, September 2022, available at: https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/

[29] Ibid.

CitizenLab has also reported that it is **likely that Hungary is also using the Candiru spyware** (now known as **Saito tech**). The company sells spyware to government customers, including 'solutions' with the capacity to spy on computers, mobile devices, and cloud accounts.[30]

Before the Pegasus scandal, Hungary was suspected of using spyware. Several civil society organizations claimed that the authorities have purchased potentially invasive surveillance technologies in the past. In 2015, files leaked from the **Hacking Team** revealed that the Hungarian government was a client.[31]

3.4. Poland

In 2018, CitizenLab reported that the **Pegasus spyware was used in Poland**. In 2021, further claims emerged that the spyware had been used against Polish journalists, including Tomasz Szwejgiert[32], prosecutors such as Ewa Wrzosek[33], lawyers, including Roman Giertych[34] and Krzysztof Brejza[35], a senator from the opposition Civic Platform (Platforma Obywatelska - PO), as well as other politicians[36]. In none of these cases had the victims been criminally charged. Critics affirmed that their surveillance was politically motivated, targeting mainly political opponents of Law and Justice (Prawo i Sprawiedliwość – PiS), the ruling party in Poland, or government critics, activists and independent lawyers. In addition, on February 7, 2022, the Supreme Audit Office (NIK) revealed that between 2020-2021, 544 of its employees' devices were under surveillance in over 7 300 attacks. According to NIK experts, three of the phones could have been infected with Pegasus[37].

While the Polish government had **initially denied** the acquisition of the spyware, **it confirmed** in early 2022 that it was in possession of Pegasus. However, the government rejected claims that the software

---

30 CitizenLab, Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus, July 2021, available at: https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

31 Freedom House, Freedom of the Net 2022, Hungary, available at: https://freedomhouse.org/country/hungary/freedom-net/2022

32 Szwejgiert was a journalist and alleged former associate of the CBA, hacked while co-authoring a book about Mariusz Kaminski, head of the CBA. See: Gera, Vanessa (25 January 2022). "Two more Poles identified as victims of hacking with spyware". AP NEWS. available at: https://apnews.com/article/technology-europe-poland-hacking-spyware-4a410bda35df566632703e3578e5a99d

33 Wrzosek was a prosecutor who challenged the PiS government's attempts to purge the judiciary. See: Gera, Vanessa (20 December 2021). "AP Exclusive: Polish opposition duo hacked with NSO spyware". AP NEWS. available at: https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e

34 Giertych was a lawyer representing top opposition politicians, and the Deputy Prime Minister in Kaczyński's Cabinet 2006–2007. See: Bajak, Frank; Gera, Vanessa (20 December 2021). "AP Exclusive: Polish opposition duo hacked with NSO spyware". AP NEWS. available at: https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e

35 Brejza was an attorney and at the time, a Civic Platform MP who ran the Civic Coalition campaign, and won his Senate seat. See: Bajak, Frank; Gera, Vanessa (23 December 2021). "AP Exclusive: Polish opposition senator hacked with spyware". AP NEWS. available at: https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab; See also: Gera, Vanessa (6 January 2022). "Rights group verifies Polish senator was hacked with spyware". AP NEWS. available at: https://apnews.com/article/technology-business-canada-elections-europe-908b0dea290ca6be1894b89f784eac60

36 Including: Michał Kołodziejczak, a farmer and leader of the social movement Agrounia; Adam Hofman, former PiS spokesman; Dawid Jackiewicz, former PiS Treasury Minister in the Cabinet of Beata Szydło; Mariusz Antoni Kamiński, former PiS MP; Bartłomiej Misiewicz, former head of the PiS cabinet and former spokesman of the Ministry of National Defence; Katarzyna Kaczmarek, wife of Tomasz Kaczmarek, former policeman and former CBA officer, later a PiS MP.

37 Wroński, Paweł; Tynkowski, Marcin (7 February 2022). "Cyberatak na Najwyższą Izbę Kontroli. "Mamy podejrzenie włamania Pegasusem na trzy telefony"" [Cyber attack on the Supreme Audit Office. "We have a suspicion of a Pegasus hacking on three phones"]. Gazeta Wyborcza (in Polish). Available at: https://wyborcza.pl/7,75398,28081346,cyberatak-na-najwyzsza-izbe-kontroli-dzis-poznamy-szczegoly.html?disableRedirects=true

had been used against opposition politicians during the 2019 parliamentary election campaign[38]. The leader of Poland's ruling party, Jaroslaw Kaczynski, stated that security services in many countries have used the software to combat crime and corruption and stressed that any use of Pegasus was "*always under the control of a court and the prosecutor's office*"[39].

On January 12, a **special committee of the Polish Senate** was established to look into the use of Pegasus[40]. The committee has so far questioned, among others, the victims of the surveillance, Citizen Lab experts, the president of the Supreme Chamber of Control (NIK) Marian Banaś, the former head of the NIK, senator Krzysztof Kwiatkowski and Wojciech Hermeliński, the former head of the State Electoral Commission, who stated that the surveillance of MP Brejza (former chief of staff of the largest party, Civic Platform) during the election campaign, could have influenced the outcome of the parliamentary elections[41].

3.5. Germany

In 2021, an investigative report conducted by two of Germany's biggest newspapers and two of its public radio broadcasting stations (Die Zeit, Süddeutsche Zeitung, WDR and NDR) found that the Federal Government had secretly **purchased the Pegasus spyware**, allegedly using it in criminal investigations of terrorism and organised crime since March 2021[42]. However, the government purchased a **technically limited variant** of the Pegasus spyware, in order to limit the possibility of abuse of existing German law. At the beginning of 2021, the German Federal Criminal Police Office (Bundeskriminalamt - BKA) used Pegasus in half a dozen cases of **suspected terrorism and organized crime**[43].

The **BKA admitted buying** Pegasus spyware in a session of the Interior Committee of the Bundestag[44]. The BKA confirmed that it had originally started talking to an NSO delegation in 2017 and made their **first purchase in 2019**.[45] It appears that the Central Office for Information Technology in the Security Sector (Zentrale Stelle für Informationstechnik im Sicherheitsbereich - ZITiS) was not involved in the procurement of the software.

---

38 Euronews, "Poland's Kaczynski admits country bought Pegasus but denies spying on opponents" (10.01.2022), available at: https://www.euronews.com/2022/01/07/poland-s-kaczynski-admits-country-bought-pegasus-but-denies-spying-on-opponents

39 Euronews. "Poland's Kaczynski admits country bought Pegasus but denies spying on opponents", (10.01.2022) available at: https://www.euronews.com/2022/01/07/poland-s-kaczynski-admits-country-bought-pegasus-but-denies-spying-on-opponents

40 Politico. "Polish leader under fire over Pegasus hack scandal", (18.01.2022) available at: https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/

41 Polishnews. "Pegasus in Poland. Former judge of the Constitutional Tribunal, Wojciech Hermeliński, on the Senate committee: this could have had an impact on the election result" (26.01.2022), available at: https://polishnews.co.uk/pegasus-in-poland-former-judge-of-the-constitutional-tribunal-wojciech-hermelinski-on-the-senate-committee-this-could-have-had-an-impact-on-the-election-result/

42 Tagesschau. " Das BKA und die umstrittene Spionage-Software" (07.09.2021), available at: https://www.tagesschau.de/multimedia/video/video-915103.html

43 Biermann, Kai, in Die Zeit, "BKA hat NSO-Spähtrojaner bereits mehrfach eingesetzt" (07.09.2021) available at: https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel

44 Süddeutsche Zeitung. "Bundeskriminalamt verwendet "Pegasus" (07.09.2021), available at: https://www.sueddeutsche.de/politik/cybersicherheit-bundeskriminalamt-verwendet-pegasus-1.5404002

45 Biermann, Kai, in Die Zeit, "BKA hat NSO-Spähtrojaner bereits mehrfach eingesetzt" (07.09.2021), available at: https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel

In the beginning of October 2021, it was also made public that the **German foreign intelligence service**, the Federal Intelligence Service (Bundesnachrichtendienst - BND), also bought an adapted version of the controversial software in a process classified as "confidential"[46].

Both, the BND and BKA stated that they could rule out that Israel (where NSO is based) is able to gain insight into the surveillance operations, but according to former NSO employees, the captured data also flowed through NSO servers[47]. The government did not want to comment on Pegasus or similar programmes used by German authorities.

The German Federation of Journalists demanded information from the German security authorities and secret services as to whether the Pegasus spyware was used against German journalists, and has called for assurances that confidential sources have not been compromised[48]. Amnesty International called for a complete investigation, stronger parliamentary control of the secret services and a review of the far-reaching powers of covert surveillance. The organisation also called for the acquisition and use of new surveillance technologies to be approved by an independent control body in the future. [49]

Already in 2012 and 2013, both the BKA and the LKA Berlin purchased FinFisher spyware from the Munich-based FinFisher Group. Given that the spyware was more advanced than what was allowed by German law, FinFisher had to rework the product for five years in order to comply with the German legal requirements and to be approved to be used[50]. The BKA paid EUR 325 666 for the spyware[51].

In principle, the BKA was only allowed to use FinSpy from 2018. In the same year, the spyware appeared on devices of members of the opposition in Turkey. By then, the contract between FinFisher and the LKA Berlin had already been cancelled[52].

In 2015, a licensing requirement was introduced throughout Europe for exports of surveillance software to countries outside the EU. The German government, in response to parliamentary inquiries, confirmed on 19 June 2019 that it has not issued an export permit for FinSpy since the licensing requirement was introduced. However, IT analyses have shown that the software samples found in Turkey in 2017 are a FinSpy version that was produced after the licensing requirement was introduced. This suggests that FinFisher exported the software illegally despite the existing requirements[53].

After the Society for Freedom Rights e.V., Reporters Without Borders (RSF), the European Center for Constitutional and Human Rights (ECCHR) and netzpolitik.org registered a criminal complaint due to

---

46 Start, Holger, in Die Zeit, "Bundesnachrichtendienst setzt umstrittene Cyberwaffe ein" (08.10.2021), available at: https://www.zeit.de/politik/deutschland/2021-10/pegasus-spionage-software-bnd-kaeufer-einsatz-israel

47 Ibid.

48 Deutscher Journalistenverband, "DJV fordert Aufklärung über Spähsoftware Pegasus" (19.07.2021), available at: https://www.djv-bawue.de/2021/07/19/djv-fordert-aufkl%C3%A4rung-%C3%BCber-sp%C3%A4hsoftware-pegasus/

49 Amnesty International, " Pegasus-Enthüllungen: Amnesty fordert überfällige Regulierung von Spähsoftware" (18.07.2022), available at: https://www.amnesty.de/allgemein/pressemitteilung/pegasus-enthuellungen-amnesty-fordert-regulierung-von-spaehsoftware

50 Meister, Andre, "Wir verklagen das BKA auf den Staatstrojaner-Vertrag" (20.07.2021), available at: https://netzpolitik.org/2021/finfisher-wir-verklagen-das-bka-auf-den-staatstrojaner-vertrag/#netzpolitik-pw

51 Krempl, Stefan, "Staatstrojaner: BKA zahlte 325.666 Euro an FinFisher" (02.08.2022), Heise Online, available at: https://www.heise.de/news/Staatstrojaner-BKA-zahlte-325-666-Euro-an-FinFisher-7200011.html

52 Ibid.

53 Gesellschaft für Freiheitsrechte, available at: https://freiheitsrechte.org/en/themen/digitale-grundrechte/export-von-uberwachungssoftware

illegal exports of surveillance software, the FinFisher group has ceased operations and is now insolvent[54].

3.6. France

There is **no indication that France has acquired the Pegasus spyware**. The country was **reported to be in negotiations with the NSO group to acquire Pegasus** when the consortium of journalists in collaboration with Amnesty International broke the news about the use of the spyware. The fallback of the allegation, especially the news that French politicians, including President Emmanuel Macron, were targeted by Pegasus allegedly stalled the negotiation and no purchase followed.[55]

As such, France does not appear to have been using Pegasus or equivalent spyware. The ensuing journalistic investigation revealed that a high number of people were targeted with the Pegasus spyware, mainly politicians and journalists. In all cases, the suspected operator are the **Moroccan secret services**. Surveillance targeted politicians in power (14 ministers are alleged to have had their phone infected[56]) as well as journalists having either openly called for greater freedom of the press in Morocco or specifically published inquests on the country[57].

3.7. Italy

Italy does not appear to have acquired the Pegasus spyware. Furthermore, there does not appear to be instances of high-profile cases where Pegasus or equivalent spyware has been used in the country. The one exception is former Prime Minister and European Commission President **Romano Prodi**, who is alleged to have been targeted with Pegasus. The revelation came in 2021, when the Washington Post reported that Mr Prodi's phone had been infected by Pegasus at the behest of the Moroccan secret services. Mr Prodi was the **UN's special envoy to Sahel**,[58] related to the issue of Western Sahara, a disputed territory between Morocco and the Sahrawi Arab Democratic Republic.

Interestingly, Italy appears to be a country in which a number of spyware vendors have established. The most famous example being **Hacking Team**. In August 2022, a consortium of international journalists under the umbrella of Lighthouse Report broke the news that **Tykelab**, a firm based in Italy belonging to **RCS Lab,** had developed products able to track mobile phone users anywhere in the world.[59] **Cy4gate,** a company set up in Italy in 2014, is another Italy-based spyware company. It offers "cybersecurity, wiretapping services for international police, and broad-spectrum intelligence". As of 2021, the company was supplying the **UAE, Saudi Arabia, Pakistan, Qatar, countries in central Asia and Latin America**. The company offers two main products: D-SINT a system that monitors social media and other databases to extract information using artificial intelligence algorithms, and of greater

---

[54] Business & Human Rights Resource Center, "Finfisher stellt nach Strafanzeige gegen illegalen Export von Überwachungssoftware Geschäftsbetrieb ein" (28.03.2022), available at: https://www.business-humanrights.org/de/neuste-meldungen/finfisher-stellt-nach-strafanzeige-gegen-illegalen-export-von-%C3%BCberwachungssoftware-gesch%C3%A4ftsbetrieb-ein/

[55] As reported in the MIT Technology Review, available at: https://www.technologyreview.com/2021/11/23/1040509/france-macron-nso-in-crisis-sanctions/

[56] Salvi, Ellen, in Mediapart, « Projet Pegasus » : Emmanuel Macron a été ciblé par le Maroc, 20 July 2020, https://www.mediapart.fr/journal/france/200721/projet-pegasus-emmanuel-macron-ete-cible-par-le-maroc

[57] Mediapart, « Projet Pegasus » : Mediapart a été espionné par le Maroc, 19 July 2021, https://www.mediapart.fr/journal/international/190721/projet-pegasus-mediapart-ete-espionne-par-le-maroc

[58] https://www.repubblica.it/politica/2021/07/21/news/spyware_pegasus_intercettato_anche_romano_prodi-311096215/

[59] Lighthouse Reports, Revealing Europe's NSO, August 2022, available at: https://www.lighthousereports.nl/investigation/revealing-europes-nso/ .

relevance Epeius. The latter is a wiretapping system able to take control of smartphones and extract private information.[60] **Grey Heron**, a firm with alleged links to Hacking Team is another example. In 2018, it offered malware designed to steal data from Telegram and Signal[61].

3.8. Netherlands

In 2018, CitizenLab found suspected NSO Pegasus infections in 45 countries, including the Netherlands.[62]

Dutch newspaper de Volkskrant reported in June 2022 that the **Dutch General Intelligence and Security Service** (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) has allegedly been using the **Pegasus** hacking software[63]. According to the news outlet, after the murder of lawyer Derk Wiersum in 2019, then Justice and Security Minister Ferd Grapperhaus asked the AIVD for help in locating Ridouan Taghi, a high-profile criminal and the main suspect in the trial. Wiersum was a lawyer for State witness Nabil B. in the Marengo case against the so-called 'Mocro Maffia' led by Ridouan Taghi[64]. Although the tracing of a criminal is not within the remit of AVID, the service helped the police in tracking Mr Taghi.[65]

Even though the use of Pegasus was legal and activated against a wanted person, the case sparked a public debate on **why the secret service was involved in an internal Dutch police investigation**, and led to demands for the re-examination of the manner in which the spyware was used in the Netherlands[66].

[60] IRPI media, Cy4gate: the Italian surveillance company seeking to challenge NSO and Palantir, December 2021, available at; https://irpimedia.irpi.eu/en-surveillances-cy4gate/

[61] Motherboard, New Spyware Company 'Grey Heron' Is Linked to Hacking Team, March 2018, available at: https://www.vice.com/en/article/bjpnad/grey-heron-hacking-team

[62] CitizenLab, HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[63] Modderkolk, Huib, in de Volkskrant, "AIVD gebruikt omstreden Israëlische hacksoftware" (02.06.2022), available at: https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/

[64] BBC News, "Dutch gangster case: Shock at murder of lawyer Derk Wiersum" (18.09.2019), available at: https://www.bbc.com/news/world-europe-49740366

[65] Security Week, Dutch Used Pegasus Spyware on Most-Wanted Criminal: Report, June 2022, available at: https://www.securityweek.com/dutch-used-pegasus-spyware-most-wanted-criminal-report

[66] Haaretz news, "Pegasus Spyware Maker NSO Has 22 Clients in the European Union. And It's Not Alone" (09.08.2022), available at: https://www.haaretz.com/israel-news/security-aviation/2022-08-09/ty-article/.premium/israeli-spyware-maker-nso-has-22-customers-in-12-eu-countries-and-its-not-alone/00000182-8403-df1d-a3a7-ae9bce800000

4. LEGAL FRAMEWORK FOR USE AND ACQUISITION

This chapter describes the existing **legal framework** in the selected Member States with regards to the **acquisition** and **use** of Pegasus and equivalent surveillance spyware, as well as any particular issue related to specific law enforcement agencies or security services (including intelligence services). It also provides information on the sanctions and remedies in case of illegal use. Where relevant, the main intelligence agencies and their role are presented.

At the **international level**, the export of spyware is regulated by the non-binding **Wassenaar Arrangement**, to which all EU Member States bar Cyprus are party. The Arrangement was amended in 2012 and 2013 to expand its coverage to include technology under the following terms: 'intrusion software', 'mobile interception or jamming equipment' and 'Internet Protocol (IP) network surveillance systems'.[67] Supporting guidance on the Wassenaar Arrangement further states that export licences should not be issued to a private company if their product may "be used for the violation or suppression of human rights and fundamental freedoms".[68]

At the **EU level**, dual-use exports are governed by **Regulation 2021/821** setting up a Union regime for the control of exports, transfer, brokering and transit of **dual-use items**[69]. The Regulation builds on previous legislation by modernising and updating the list to technologies covered by export controls, in particular in the field of emerging technologies.

The Wassenaar Arrangement is not legally binding, while there are "divergent interpretations and applications"[70] at national level of the terminology used in the Arrangement. In the EU, Regulation 2021/821 allows Member States to address the risk of human rights violations linked with trade in cyber-surveillance technologies. It also enhances the EU's capacity to control the flow of trade in sensitive new and emerging technologies. However, given its recent implementation, it is not possible to assess its effectiveness.[71]

4.1. Greece

Hacking and the use of spyware is illegal in Greece. The Greek **Criminal Code** defines **hacking** as the unauthorised access to electronic data, which carries a **penalty** of up to two years imprisonment (art. 370B(1), the unauthorized access to information systems or to information transmitted through telecommunications systems, which carries a penalty of up to five years' imprisonment (art. 370D(2). Aggravating circumstances when hacking includes the severe hindrance to the operation of an information systems or when data is modified or supressed as a result of the hacking. Attempting to fraudulently acquire sensitive personal information through deception also warrant a penalty of up to

---

67 Bauer, S. and Bromley, M. 2016. The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World. Non-Proliferation Papers by the EU Non-Proliferation Consortium. No. 48.

68 The Wassenaar Arrangement – On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, About Us. http://www.wassenaar.org .

69 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)

70 Immenkamp, B (European Parliamentary Research Service), 2017. Review of dual-use export controls: European Parliament Briefing: EU Legislation in Progress, available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

71 See Portolano Cavallo, European Union adopts new regulation no. 2021/821 on dual use, 2021, available at: https://portolano.it/en/newsletter/portolano-cavallo-inform-compliance/european-union-adopts-new-regulation-no-2021821-on-dual-use.

five years' imprisonment (art. 386(1)), which can rise to up to 10 years if the damage induced as a result of phishing exceeds EUR 120 000.

In December 2022, the parliament passed a law banning the sale and use of spyware by private individuals. The penalty if a prison sentence of 10 years'. The law further restricts the use of spyware against politicians to cases of national security.[72]

Infecting an IT system with malware (including **spyware**) is a criminal offence and covered by different articles of the criminal code depending on the type of infection. This includes art. 292 on crimes against the security of telephone communications, art. 292B on hindering the operation of information systems, art. 370 on the violation of the secrecy of letters.

The possession or use of spyware to commit cybercrime is criminalised by article 292C of up to two years imprisonment. The **production, sale, supply, use, importation, possession, distribution** of programmes designed as malware (including spyware as defined in art. 292B) is criminalised by art. 292C of the penal code.[73] It carries a custodial sentence of up to two years.

The Ministry of foreign affairs is responsible for authorising the export of dual-use goods (General Secretariat of International Economic Relations and Openness).

In procedural law, "**special investigative techniques**" are allowed. According to the main Executive Law 2225/1994[74], communications secrecy may be waived for reasons of **national security** (Article 3) or for the purposes of identifying certain **criminal offences** (Article 4). Lifting of confidentiality is also permitted in order to investigate felony and misdemeanour (article 153 of the code of criminal procedure). Certain crimes referred to in Article 254 of the Hellenic Criminal Procedure Code[75] (organised crimes, counterfeiting, human trafficking, rape and sexual abuse of a minor, child pornography) are explicitly mentioned as crimes warranting special investigative techniques. Corruption investigations are also included and covered by a separate article of the code of criminal procedure (article 255).

In order for the police to be able to use these techniques, a **judicial order** must have been issued by the prosecutor of the Court of Appeal. In cases of serious crime, a judicial council is competent to issue the order.

Once the order is granted, a copy must be handed to the president, administrative council, general director or representative of the legal entity responsible for waiving confidentiality, as well as to the Hellenic Authority for Communication Security and Privacy.[76]

The state organisations which are allowed to use special investigative techniques include:

- The **National Intelligence Service** (*Ethnikí Ypiresía Pliroforión* – EYP) – which is the country's national intelligence agency subject to the authority of the Prime Minister (following a change of law in 2019) and is responsible for both foreign and domestic intelligence gathering. The agency is

[72] The Guardian, Greece passes intelligence bill banning the sale of spyware, available at: https://www.theguardian.com/world/2022/dec/09/greece-passes-intelligence-bill-banning-the-sale-of-spyware

[73] ICGL, Cybersecurity Laws and Regulations 2022, chapter on Greece, available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/greece

[74] Law 2225/1994 for the protection of freedom of correspondence and communications and other provisions. ('Για την προστασία της ελευθερίας της ανταπόκρισης και άλλες διατάξεις') (O.G.A' 121/20.07.1995).

[75] Article 254 of the Code of Criminal Procedure, available at: https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4620-2019/arthro-254-kodikas-poinikis-dikonomias-nomos-4620-2019

[76] FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, Greece, October 2014, p. 18.

a civilian agency directly under the authority of the Prime Minister who is responsible for the appointment of dismissal of the agency's director;

- The **Hellenic Police Intelligence Division** (*Διεύθυνσης Διαχείρισης και Ανάλυσης Πληροφοριών* - HPiD) constitutes an independent central service acting as a central point for intelligence in the Hellenic Police. It is the intelligence Hub of the Hellenic Police, focusing on combating all forms of crime, but mainly Serious and Organised Crime and Terrorism.

Law 3649/2008 on the National Intelligence Service sets out the way in which the intelligence services can use special investigative techniques. They are allowed for national security purposes (articles 3 and 5). A Public Prosecutor assigned to the EYP must approve the request to use special investigative techniques. Following the Predator revelations, on 9 August 2022, the government introduced an Act of Legislative Content, reinstating the two-prosecutor authorisation for surveillance operations – abolished by the previous government in 2018 – and introducing a hearing and opinion by the competent parliamentary committee before appointing the EYP Director..[77]

4.2. Spain

The Spanish **Constitution** recognises the right of privacy of communications including the confidentiality of "postal, telegraphic and telephone communication" (Section, 18 (3)).

The **Criminal Code criminalises** a number of actions related to the **use** and **acquisition** of spyware. According to article 197, whoever seizes "*electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or image, or any other communication signal*", is liable to a **prison sentence of up to four years**.

Article 264 ter states that '*whoever, without being duly authorised, produces, acquires for use, imports or, in any way […] provides third parties with' a programme, password an access code or similar data enabling access to all or part of an information system […] shall be punished* with a prison sentence of six months to two years in prison or a fine of three to eighteen months (of the person's salary).

Article 264 criminalises the erasure, damage, deterioration, alteration, suppression or making inaccessible data, computer programmes or electronic documents. However, the article does not criminalise the fact of gaining access to document or communications.

In some cases, set out in in Part I, Chapter V of the Constitution, some rights and freedoms can be suspended. Section 55(2) refers to the suspension of some rights for individuals subjected to investigations of the activities of armed bands or terrorist groups. It does however require "*necessary participation of the courts and proper parliamentary control*"[78].

The Criminal Procedure Act also provides some detail on investigations affecting the rights enshrined in Article 18 of the constitution (i.e. right to privacy). The "***interception*** *of telephone and telematic communications, capture and recording verbal communications with the use of electronic devices, use of technical devices for image surveillance, location and capture, search of mass data storage devices and remote searches of computer equipment*" is allowed in the Act if a **judicial authorisation is issued by a judge** (art 588 a. ii), and fully subject to the following principles (art. 588 a. i.):

---

[77] Iefimerida, Σαρωτικές αλλαγές στην ΕΥΠ: Η ΠΝΠ με τις ρυθμίσεις που ενισχύουν τη διαφάνεια -Με 2 υπογραφές εισαγγελέων οι παρακολουθήσεις, August, 2022, available at: https://www.iefimerida.gr/politiki/sarotikes-allages-stin-eyp-praxi-nomothetikoy-periehomenoy

[78] Spanish Constitution, Part I, Chapter V, Section 55(2).

- **speciality**: the measure is related to a specific crime;
- **adequacy**: setting out the objective and subjective scope as well as the duration on the measure;
- its **exceptional nature** and **necessity**; no other measure is available, or the investigations would be hampered without the measure), necessity and proportionality of the measure;
- **proportionality**: which includes the severity of the case, its social transcendence or the technological field of production, the strength of existing prima facie evidence and the relevance of the result sought.

These principles apply to all interceptions listed above, as well as the interception of telephone and telematic communications and extended to any two-way telematic communication system - such as WhatsApp, SMS and covert listening devices.[79]

The Spanish intelligence community is made up of three main organisations:

- the **National Intelligence Service** (Centro Nacional de Inteligencia, CNI), which acts as both a domestic and foreign intelligence service. The CNI is under the control of the Ministry of Defence (reflecting its history as the Higher Centre for Defence Intelligence, which it replaced in 2002). The Director of the service is appointed by the King at the proposal of the Minister of Defence. The Director has a specific relationship with the Prime Minister, being its main advisor for intelligence and counter-intelligence;[80]
- The **Intelligence Center for Counter-Terrorism and Organized Crime** (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, CITCO), the domestic intelligence agency responsible in particular for terrorism, organised crime and violent radical organisations;
- The **Spanish Armed Forces Intelligence Center** (Centro de Inteligencia de las Fuerzas Armadas, CIFAS), the defence intelligence agency; under the Ministry of Defence and Prime Minister.

As mentioned in section 3.2, the **CNI was responsible for the use of spyware targeting journalists, lawyers, human rights defenders and political representatives**. The CNI was established by law 11/2002 that authorises it to carry out "security investigations", without specifying the mechanism or the limits of such investigations.[81]

In Spain, the General Secretariat for Foreign Trade (Secretaría General de Comercio Exterior), the Customs Department (Agencia Tributaria - Aduanas) and the Foreign Office Ministry (Ministerio de Asuntos Exteriores, Unión Europea y Cooperación) are the authorities empowered to grant licences and to decide to prohibit the transit of dual-use items.

4.3. Hungary

The Hungarian **criminal code** contains a chapter on **illegal data acquisition** and criminal **offences against information systems**.[82] It covers the illegal data acquisition, in particular a "*person who, for the purpose of gaining knowledge of any personal data, personal secret, economic secret or trade secret without authorisation:…*

[79] FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, July 2016.

[80] See CNI website, available at: https://www.cni.es/en/about-the-cni/controls-of-the-cni

[81] OMCT, Spain: State surveillance on journalists, politicians, and lawyers, May 2022.

[82] Act C of 2012 on the Criminal Code (as in force on 1 April 2022), available (in English) at: https://njt.hu/translation/J2012T0100P_20220401_FIN.pdf

- (b) *surveils or records the events taking place in the home of another person or any other related premises or a fenced area of them by using technical means in secret …*
- *(d) intercepts in secret, and records, by using technical means, any communication conducted through an electronic communications network or device or an information system,…*
- *(e) intercepts in secret, and records, by using technical means, any data processed in an information system"*

These crimes are punished by **up to three years' imprisonment** (section 422).

Spyware is covered by section 423 (1) which punishes of **up to two years' imprisonment** a person who "*logs into an information system without authorisation by violating or circumventing a technical measure safeguarding that information system*".

The law does allow for some bodies to use **special investigation techniques** to collect information for specific reasons.

The **Police Act**, which regulates the role of the police in the country contains provision relating to criminal investigations. According to the act, the surveillance of private citizens can only be carried out with **judicial approval**. In matters of **terrorism**, however, the Police Act refers to the investigatory surveillance mentioned in the National Security Act.[83] Under this provision, judicial approval does not have to be sought to approve the use of these techniques Instead the Minister of Justice is responsible for providing the authorisation..[84]

The **National Security Service** are entitled to *(a) search a dwelling secretly and record by means of technical equipment what they perceive; b) keep a dwelling under surveillance by means of technical equipment and record what they perceive; c) open and check postal mail and any closed parcel belonging to an identifiable person and record their contents by means of technical equipment; d) detect the content of communications transmitted by electronic communications network and record it by means of technical equipment; e) detect the data transmitted by or contained on a computer or network, record it by means of technical equipment and use it."* (Section 56 of the National Security Act)[85].

In a landmark case (*Szabó and Vissy v. Hungary*[86]), the European Court on Human Rights (ECtHR) found that Hungary had violated the right to respect for private and family life protected by article 8 ECHR. In the judgment, the court found that while there was a legal basis for the surveillance of the defendants, the **Hungarian legislation on secret surveillance measures did not provide for safeguards sufficiently precise, effective and comprehensive** on the ordering, execution and potential redressing of such measures. However, despite the judgement, **the Hungarian government has so**

[83] FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary, 2014.

[84] FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary, legal update, 2016.

[85] Hungary, Act CXXV of 1995 on the National Security Services (A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény).

[86] Szabó and Vissy v. Hungary, application no 37138/14, judgment of 12 January 2016, available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}

far failed to adapt the country's legislation to increase protection against unjustified secret surveillance in the name of national security.[87]

While the National Security Act refers to "National Security Services", no one agency in Hungary is called as such. Instead, the terms is understood to **comprise five organisations** in addition to the counter terrorism organisation mentioned before[88]:

- the **Information Office** (*Információs Hivatal*), under the authority of the Prime Minister's office;
- the **Constitution Protection Office** (Alkotmányvédelmi Hivatal), under the authority of the Minister of the Interior;
- the **Military National Security Service** (Katonai Nemzetbiztonsági Szolgálat) under the authority of the Ministry of Defence;
- the **Counter-Terrorism Information and Criminal Analysis Centre** (*Terrorelhárítási Információs és Bűnügyi Elemző Központ, TIBEK),* which was established for the collection and systematisation of information and the outcomes of surveillance operations gathered by the various national security services in order to inform decision makers on further measures to implement); *and*
- the **Special Service for National Security** (SSNS, *Nemzetbiztonsági Szakszolgálat - NBSZ),* which can provide assistance for other security services to gather intelligence.

The authorisation of the special investigative techniques requires the **prior authorisation from a judge, the Minister of Justice, or the general directors of the National Security Services**.[89]

In Hungary, the Government Office of the Capital City Budapest Department of Trade, Defence Industry, Export Control and Precious Metal Assay Export Control Unit is responsible for authoring the export of dual use items.

4.4. Poland

The Polish constitution recognises the right to privacy (article 47) and the freedom and privacy of communication (article 49).

The phenomenon of **hacking** is presented and penalised as a crime through the **Polish Criminal Code**.[90] Article 267 of the Criminal Code provides for several offences, defining them as:[91]

i. *Whoever without authorisation obtains access to an information not meant for them, by opening a sealed letter, connecting into a telecommunications network, or by breaking or avoiding electronic, magnetic, informatic or other special protection of such network shall be punished by imprisonment of up to two years.*
ii. *The same penalty shall apply to anyone who without authorization obtains access to the whole or a part of an informational system.*

[87] Hungarian Civil Liberties Union (HCLU), Communication under Rule 9.2 of the Rules of the Committee of Ministers regarding the supervision of the execution of judgments and terms of friendly settlements by the Hungarian Civil Liberties Union, January 2022.

[88] FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary, legal update, 2016, p 6.

[89] FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary, legal update, 2016.

[90] Polish Penal Code: Act of 6 June 1997.

[91] Polish Penal Code: Act of 6 June 1997, art. 267. *Unofficial translation provided by study expert, Ivan Skorvánek.*

iii. *The same penalty shall apply to whoever with an aim of obtaining information to which they are not authorized uses eavesdropping, visual or other tools or programs.*
iv. *The same penalty shall apply to whoever reveals information obtained by means described in 1-3 to another person.*
v. *Offences described in 1-4 are prosecuted upon the request of the victim.*

Anyone convicted of hacking is liable to a **fine of up to PLN 1.08 million (EUR 2.3 million),, restriction of liberty or imprisonment for up to two years**[92]. The same is applicable to anyone who acquires access to any part of a computer system without being authorised to do so.

If unauthorised access to information includes information constituting personal data, a violation of the **GDPR** is also likely; this has a **penalty** of **up to EUR 20 million** or, in the case of an enterprise, up to **4%** of its total annual global turnover (whichever is higher)[93]. The law enforcement Directive is also relevant, although the law transposing the Directive[94] has incorrectly exempted all statutory activities of the Central Anticorruption Bureau from the scope of the data protection. However, not all activities of the Central Anticorruption Bureau are covered by national security (an exemption allowed by law enforcement directive).

Phishing is included as a criminal offence under Section 287 of the Polish Criminal Code, which states that anyone who, in order to achieve material benefits or to inflict damage upon another person, affects the automatic processing, collection or transmission of data or changes, deletes or introduces new entries, without being authorised to do so, is liable to **imprisonment for up to five years**. If phishing leads to identity theft or fraud, it may also be considered an offence under Section 190a of the Polish Criminal Code.

In addition, **infecting IT systems with malware (including ransomware, spyware, worms, trojans and viruses)** is a criminal under Section 287 of the Polish Criminal Code (similar to Phishing). According to Section 269 of the Polish Criminal Code, anyone who destroys, deletes or changes a record on a computer storage media that is of particular significance for national defence, transport, safety or the operation of the government or any other state authority or local government, or that interferes with or presents the automatic collection and transmission of such information, is liable to **imprisonment for up to eight years**.

The **distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime**, are criminal offences under Section 269b. Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit cybercrime (e.g. damaging, databases, preventing automatic collection and transmission of data, or hindering access to data) is liable to imprisonment for up to five years.

Anyone who **creates, obtains, transfers or allows access to hardware or software adapted to commit cybercrime**, including computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network, is liable to imprisonment for up to three years.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points) is a criminal offence under Section 267 of the

[92] ICLG, Cybersecurity Laws and Regulations 2022 – Poland, available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/poland

[93] Ibid.

[94] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000125

Polish Criminal Code. If someone who is not authorised to do so, acquires access to information not intended for him and her, by, inter alia, connecting to a cable transmitting information or by breaching electronic, magnetic or other special protection for that information, is liable to a fine (up to PLN 1.08 million), restriction of liberty or imprisonment for up to **two years**. This also applies to anyone who acquires access to any part of a computer system without being authorised to do so. Unsolicited penetration testing may also constitute a criminal offence under Section 266 of the Polish Criminal Code – Electronic theft.

Unser Section 165, subsect. 1 point 4 of the Polish Criminal Code, anyone who puts the lives of health of many people or possessions in danger by affecting computerised data commits a separate crime and may be sentenced for up to **eight years** of imprisonment. If any offence is committed due to or in relation to the offences listed above, the offender may be found guilty of committing several offences by one act; if the offence is related to terrorism, the punishment may be even more severe.

The use of special investigative techniques is allowed by the **Code of Criminal Procedure**[95]. It covers elements such as programmes that can compromise all data present on one' mobile device by including a separate legal regime on surveillance for criminal investigations. For example, **Chapter 26 of the Code** regulates wiretapping and recording of telephone or online communications via other technical means[96]. However, many of the core functions of spyware such as Pegasus, including those that could potentially lead to a large-scale gathering of biometric data, are outside the regulatory oversight of the Code.

In 2016, Poland's ruling Law and Justice Party (PiS) introduced a series of amendments to the Code of Criminal Procedure. For example, **Article 168 of the Code of Criminal Procedure permits the use, in criminal proceedings, of evidence that has been obtained in violation of law** (e.g. as a result of illegal wiretapping, searches, so-called provocations, the use of torture, inhuman and degrading treatment, provided it has not resulted in health injury). According to **Article 168a of the Code of Criminal Procedure**, "*Evidence may not be considered inadmissible solely on the grounds of the fact that it has been obtained in violation of the rules of procedure or by means of a prohibited act referred to in Article 1(1) of the Criminal Code, unless the evidence has been obtained in connection with the performance by a public official of his/her personal duties with regard to a murder, wilful injury or deprivation of liberty.*"

Intelligence services can also make use of special investigative techniques. However, the framework in which these operate is wage. The following intelligence services exist in Poland[97]:

- **Internal Security Agency** (*Agencja Bezpieczeństwa Wewnętrznego*): is responsible for prevention and combating of crimes, fighting national security threats, protection of classified information. The Agency is entitled to conduct "operational control" (i.e. wire-tapping) only when fighting crimes listed in Article 5.1. point 2 of the Act on the Internal Security Agency threats. These include crimes such as espionage, terrorism, infringement of State secrets, as well as other criminal offences threatening State security[98]. The Agency is also competent to access metadata (telecommunication, internet and postal data) in order to complete the tasks mentioned in Article 5.1., which also includes general fight against national security threats;

[95] Polish Code of Criminal Procedure, Act of 6 June 1997. Unofficial translation available at: https://legislationline.org/sites/default/files/documents/f6/Polish%20CPC%201997_am%202003_en.pdf.

[96] EDRI report, p. 127.

[97] FRA. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies. Legal update, p. 2.

[98] The Act on the Internal Security Agency and Foreign Intelligence Agency of 2002.

- **Intelligence Agency** (*Agencja Wywiadu*): the tasks of the Intelligence Agency include the analysis of foreign threats to security and can be run only outside the territory of Poland.

In Poland, the Ministry of Entrepreneurship and Technology Department for Trade in Strategic Goods and Technical Safety is responsible for overseeing dual-use exports.

4.5. Germany

The German Criminal Code criminalises **hacking** (i.e. unauthorised access **and data espionage**) as unlawfully obtaining data for oneself, or another, that was not intended for one and was especially protected against unauthorised access, and circumventing protection. Once convicted, a person is liable to **imprisonment not exceeding three years, or a fine**[99]. Phishing is defined as intercepting data that are not intended for someone, without being authorised to do so, either for themselves or another, by technical means from non-public data transmission or from an electromagnetic broadcast from a data-processing facility. The penalty for such an offence is **imprisonment** for a term not exceeding **two years or a fine**, unless the offence is subject to a more severe penalty under other provisions[100]. Depending on the case, "hacking" could possibly come under the definition of both of the offences set out above, depending on the level of protection applied to the data in question.

The infection of IT systems with malware (including ransomware, **spyware**, worms, trojans and viruses) constitutes a criminal offence according to the German Criminal Code ("computer sabotage")[101]. Interfering with data-processing operations that are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, entering or transmitting data with the intention of causing damage to another, or destroying, damaging, rendering unusable, removing or altering a data-processing system or data carrier, is punishable of imprisonment for up to three years or a fine for the former, or imprisonment for up to five years or a fine for the latter[102].

The **distribution or selling of hardware, software or other instruments** being used to commit cybercrime is a crime under Sec. 27 of the Criminal Code, and this **use is covered by the seller's intent**[103]. The **possession of hardware, software or other tools** that can be used to commit cybercrime can constitute a criminal offence[104]. The preparation of the commission of data espionage or phishing by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible, software for the purpose of the commission of such an offence shall be liable to imprisonment for up to one year or a fine. In case of a use of such instruments, the same principles as set forth above with respect to "Hacking" apply.[105]

---

99 Sec. 202a StGB (*Strafgesetzbuch* – Criminal Code).

100 Sec. 202b StGB

101 Sec. 303b StGB

102 Sec. 303b StGB

103 Sec. 27 StGB

104 Sec. 202c StGB

105 Other activities with the conduct mentioned above constitute criminal offences under German criminal law: these are, for example, (i) preparing of an unauthorised obtaining or interception of data (Sec. 202c of the German Criminal Code); (ii) handling of stolen data (Sec. 202d of the German Criminal Code); (iii) violation of postal and telecommunications secrets (Sec. 206 of the German Criminal Code); (iv) computer sabotage (Sec. 303b of the German Criminal Code); (v) certain types of violation of the EU GDPR with the intention of enrichment or to harm someone (Art. 84 of the GDPW and Sec. 42 of the German Federal Data Protection Act); and (vi) falsification of digital evidence (Sec. 269 et. Seq. of the German Criminal Code).

Since 1949, the **right to privacy of correspondence, posts and telecommunications has been highly protected**, as evidenced by its prominent placement at the forefront of the German Constitution (Basic Law – *Grundgesetz* §10).[106]

The law allows for the use of special investigative techniques in criminal cases, which includes spyware.

In 2008, the **Federal Constitutional Court** made a landmark ruling (Decision BvR 370/07).[107] This decision tackled what the court reported to be the first open instance of "secret access to information technology systems" (through spyware) –.[108] The phrase "secret access to information technology systems"[109] is further explained in the ruling as "technical infiltration which for instance takes advantage of the security loopholes of the target system [i.e. system vulnerabilities], or which is effected by installing a spy program".[110] Wider debates on this topic in Germany otherwise refer to this secret access as 'online search/online surveillance' and generally discuss the intelligence community; this is discussed below.[111]

The above-mentioned Decision BvR 370/07 declared this **"secret access" (through spyware) null and void as it was determined to be incompatible** with the Basic Law.[112] The decision resulted in an evolved interpretation of the right to personality[113] that encompasses the "**fundamental right to the guarantee of the confidentiality and integrity of information technology systems**".[114] **Since then, the infiltration of mobile phones through spyware has only been permitted in Germany in exceptional cases**. Measures which merely serve to access communications, as long as they are legally and technically restricted to that purpose, are not covered by this fundamental right, but should only be measured against Art. 10 GG protecting correspondence, post and telecommunications.[115]

Decision 51, 211 of the Federal Court of Justice in Criminal Cases (*Entscheidungen des Bundesgerichtshofes in Strafsachen – BGHSt*) from 2007 further contributed to this ruling. This decision stipulated that the Code of Criminal Procedure (*Strafprozessordnung – StPO*) did not currently contain a legal basis for such "secret search".[116]

In **2017**, the Code of Criminal Procedure (*Strafprozessordnung – StPO*) was changed. With Art. 3 of the Law on more effective and practicable design of criminal proceedings (*Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens* - Federal Law Gazette I 2017, p. 3202), **a legal basis**

---

106 Art. 10 GG (*Grundgesetz* - German Basic Law).

107 BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html .

108 As stipulated in §5.2 no.11 sentence 1 alternative 2 of the Constitution Protection Act in North Rhine-Westphalia (i.e. the defendant in this case) Art. 5.2, nr.11, sentence 1, alternative 2 VSG NRW (Constitution Protection Act – North Rhine-Westphalia).

109 Ibid.

110 BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

111 Id.

112 Art. 1.1, 2.1, 10.1 & 19.1 GG.

113 Right to personality – Enshrined in Basic Law Article 2.1 in conjunction with Article 1.1 GG.

114 BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html .

115 BVerfG, Judgment of the First Senate of 27 February 2008 – 1 BvR 370/07 – paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html

116 Decisions of the Federal Court of Justice in Criminal Cases (*Entscheidungen des Bundesgerichtshofes in Strafsachen* – BGHSt) 51, 211.

was created in the StPO for **source telecommunications surveillance** as well as for **online searches**[117].

The Law on the restructuring of the Federal Criminal Police Office Act (*Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes* – Federal Law Gazette I 2017, p. 1354) of 1 June 2017 enabled the **German police** (*Bundeskriminalamt* – ***BKA***) **to use source telecommunications surveillance and online searches by court order or by order of the President of the German Police (BKA)**[118] to monitor encrypted communications and covertly search computers or mobile phones in order to avert an urgent threat to the existence or security of the Federation or a Land or to the life, limb or freedom of a person or property of significant value, the preservation of which is in the public interest, or for the defence against dangers of international terrorism[119]. For this purpose, **spy software** is installed on the device unnoticed. **The BKA has also developed several such programmes itself and has purchased other commercial products**.

The law also allows intelligence agencies to use special investigative techniques. Germany's three main intelligence agencies who have access to these techniques are:

- The **Federal Intelligence Service (Bundesnachrichtendienst – BND)** focussing on foreign and military intelligence, directly under the authority of the chancellor's office;
- The **Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz - BfV**): national domestic intelligence, which report to the ministry of the interior; and
- The **Military Counterintelligence Service (Militärischer Abschirmdienst - MAD**): the counterintelligence organisation within the Bundeswehr, Germany's army;

In addition, each of Germany's 16 Länder have security agencies (State Offices for the Protection of the Constitution - *Landesbehörde für Verfassungsschutz* – LfV).The organisation, tasks and powers of the Federal Intelligence Service (*Bundesnachrichtendienst* - **BND**) is regulated in the Federal Intelligence Service Act[120]. The BND may use intelligence resources to secretly obtain information if this is necessary to fulfil its tasks[121]. If personal data is collected from foreigners abroad, individuals are not informed[122]. In cases where the BND is active in Germany, its measures are subject to the regulations and the control according to the G-10 Act[123]. The BND law was extensively amended in December 2016, to allow for the

---

[117] "Source telecommunications surveillance" is about enabling surveillance of telecommunications originating from a system. The authority's access rights to source telecommunications surveillance are generally limited to the content of the ongoing communication (Section 100a Paragraph 5 sentence 1 no. 1a StPO). Communication data may be recorded before they are encrypted or after they have been decrypted. However, no information should be obtained that could not have been obtained and recorded during the ongoing transmission process in the public telecommunications network (Section 100a (5) sentence 1 no. 1b StPO).

The "online search" is about monitoring the system itself and collecting data from it. In online searches, a computer system is searched comprehensively or specifically so that not only communication data but all stored data can be viewed, such as chats, uploaded photos, written notes and website histories. From this, a comprehensive picture of the online behaviour of a monitored person can be assembled.

[118] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten(Bundeskriminalamtsgesetz – BKAG, 01. Juni 2017, p. 76 (available at: https://www.bka.de/SharedDocs/Downloads/DE/DasBKA/Auftrag/bkag/bkaGesetz.pdf?__blob=publicationFile&v=1

[119] Paragraph 51, Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes – Federal Law Gazette I 2017, p. 1354.

[120] *Gesetz über den Bundesnachrichtendienst* – last update in 2021, available at: https://www.gesetze-im-internet.de/bndg/index.html .

[121] Section 5 sentence 1 BNDG in conjunction with Section 8 paragraph 2 BVerfSchG).

[122] Paragraph 59, Gesetz über den Bundesnachrichtendienst.

[123] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses.

surveillance of foreign nationals located on the German territory. However in May 2020, the Federal Constitutional Court declared the amendments to the BND Act to be largely unconstitutional, since they violated the fundamental rights of telecommunications secrecy (Art. 10 Para. 1 GG) and freedom of the press (Art. 5 Para. 1 Sentence 2 GG)[124]. A new amendment of the BND law was decided on in 2021.

The Federal Constitutional Protection Act (BVerfSchG) regulates the tasks and the legal status of the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz* - BfV) as well as the cooperation of the BfV with the constitutional protection authorities of the federal states in Germany.

In accordance with the G-10 Act, the federal and state authorities for the protection of the constitution, the Military Counterintelligence Service (*Militärischer Abschirmdienst* - MAD) and the BND are entitled under certain conditions, in particular to avert imminent dangers to the free democratic basic order or the existence or security of the federal or the *Länder* governments, to monitor and record telecommunications.[125]

In July **2021**, the law "to adapt the constitutional protection law" (*Gesetz zur Anpassung des Verfassungsschutzrechts*)[126] came into force. For the first time, this law grants all 19 **German intelligence services[127] the right to use state trojans** to read ongoing communication on computers or smartphones and even past communication data. **Individual legal protection is almost impossible, since the surveillance takes place in secret and is usually not disclosed afterwards**. In addition, the law introduces a legal basis for a more elaborate information exchange between the Office for the Protection of the Constitution and the Military Counterintelligence Service (MAD) by giving the MAD access to the intelligence information system. The monitoring and recording of ongoing telecommunications must be approved by the G10 Commission, a secret committee that decides on wiretapping measures by these services.

In Germany the Federal Office for Economic Affairs and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle) is responsible for authorising dual-use exports.

4.6. France

The French Criminal Code (Code Pénal) **defines spying** as the capture, saving or transmission of voice, images and geo-localisation information without the knowledge or consent of the person targeted (art. 226-1).[128] Other relevant infractions include opening, deleting, slowing or diverting the transmission […] and obtaining the contents of the communication (art. 226-15).

The French Criminal Code criminalises **hacking** which is defined as "*to access or stay in a fraudulent manner in all or part of an automated data processing system*"[129]. The **use of spyware** is covered by article 323-3 of the criminal code. The article criminalises the "*fraudulent introduction, extraction, detention, reproduction transmission, deletion or modification of data in an automated data processing system*". The definition of spyware has been clarified in a guideline published in the official journal as "*software*

[124] BVerfG, Judgment of the First Senate of 19 May 2020 - 1 BvR 2835/17 - https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html

[125] Paragraph 1 (1) G-10 Act.

[126] Gesetz zur Anpassung des Verfassungsschutzrechts, Federal Law Gazette 2021 Part I No. 40, issued on July 8th, 2021, page 2274.

[127] The BND, BfV, MAD and the 16 LfV.

[128] Code pénal, article 226-1

[129] Article 323-1 of the French criminal code, available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2022-10-09/

designed to collect and transmit to third parties and without the knowledge of user data about the user or information relevant to the system she uses."[130] **Sanctions** can go up to three years' imprisonment and a fine of up to EUR 100 000 in the case of hacking, and EUR 150 000 for the use of spyware.

Although there is no constitutional **right to privacy** or confidentiality of communications in France, the right to privacy is provided for in Article 9 of the *Code Civil,* as well as in the Post and Electronic Communications Code (*Code des postes et des communications électroniques*) and in the domestic law application of the European Convention on Human Rights.[131] Furthermore, the right to privacy has been embodied in several decisions of the French Constitutional Court.[132]

The Criminal Code forbids the **manufacture**, **import**, **possession**, **display**, **offer**, rental or **sale** of technical equipment or devices likely to allow operations including the interception of conversations, or to install software able to do so on devices (art. 226-3). **Sanctions** can go up to five years' imprisonment and a fine of up to EUR 300 000. In France, the export of **dual-use** technologies must be authorised by a **special commission** (Commission interministérielle des biens à double usage – Cibdu). Decisions made by the Cibdu are covered by national defence secret and therefore not public.[133]

Exceptions are made for Law Enforcement Authorities who are allowed to use special investigation techniques for the investigation of specific crimes, listed in article 706-73 and 706-73-1 of the code of criminal procedure. These crimes include inter alia murder, trafficking (of human being, drugs, firearms and other weapons), theft, terrorism, money laundering. They also include facilitation of irregular immigration as part of a criminal group. **Security services** are also allowed to use such tools. Provisions on the interception of electronic correspondence by the **security services** are also included in state security law, which governs the prevention of terrorism, organised crime and organised delinquency.[134]

France has **four main intelligence agencies** which are allowed to use all intelligence gathering techniques:

- the **Directorate General of Interior Security** (*Direction générale de la sécurité intérieure* – DGSI), which encompasses civil internal security, under the direct supervision of the Ministry of Interior;
- the **Directorate General of External Security** (*Direction générale de la sécurité extérieure* – DGSE), which covers civil external security dependant on the Ministry of the Armed Forces;
- the **Directorate of Intelligence and Security of Defence** (*Direction du Renseignement et de la Sécurité de la Défense – DRSD*), which is responsible of intelligence, counter-intelligence concerning national defence, under the control of the Ministry of the Armed Forces; and
- the **National Directorate of the Intelligence and Customs Investigations** (*Direction Nationale du Renseignement et des Enquêtes Douanières – DNRED*), whose mission is to gather, centralise and

---

[130] JORF n° 0130 du 7 juin 2007, available at : https://www.legifrance.gouv.fr/download/securePrint?token=wS88ORpTT79QHotPjEKZ

[131] Korff, D., Wagner, B., Powles, J., Avila, R. and Bürmeyer, U. (2017) Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes. Global Report – January 2017, available at SSRN: https://ssrn.com/abstract=2894490

[132] See Decision no. 2009-580 DC of 10 June 2009; Decision no. 94-352 DC of 18 January 1995; Decision no. 99-422 DC of 9.11.1999; Decision no. 99-419 DC of 9.11.1999; Decision no. 99-416 DC of 23.07.1999; Françoise MONÉGER - Nouveaux Cahiers du Conseil constitutionnel n° 39 (Dossier : la Constitution et le droit des personnes et de la famille) - avril 2013.

[133] Hourdeaux, Jérôme, Mediapart, Commerce des armes numériques : la grande hypocrisie , 21 July 2021, available at : https://www.mediapart.fr/journal/international/210721/commerce-des-armes-numeriques-la-grande-hypocrisie

[134] Sieber, U. and von zur Mühlen. 2016. Access to Telecommunication Data in Criminal Justice: A Comparative Analysis of European Legal Orders. Duncker & Humblot, Berlin, pp. 441-442.

process intelligence relating to customs, including smuggling of illegal goods. It is placed under the control of the Ministry of Economics and Finance.

The surveillance powers, and thus hacking practices, of these intelligence agencies are primarily governed by the ***Loi relative au renseignement*** (n° 2015-912 of 24 July 2015), introduced in response to several terrorist attacks. This law aims to provide "a single legal framework for its intelligence gathering activities, by defining applicable principles, the different techniques that are used and by reinforcing control"[135]. The law was complemented in 2021 by a second law, the *Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement)*.[136]

The law **limits** the purposes for which hacking techniques can be operationalised and states that they must only be performed with respect to the principles of **proportionality**.[137] Furthermore, it outlines a range of additional **conditions** that must be met, similar to the case of law enforcement, (e.g. related to duration, severity of the threat, prime ministerial authorisation, etc.) and **oversight** mechanisms to ensure transparency and accountability (e.g. the Commission for Oversight of Intelligence Gathering Techniques – CNCTR, effective judicial recourse etc.).

Despite the **criticisms** levied at the 2015 law by the **European Parliament**, which was concerned that it extended the capabilities of intelligence bodies and "raised important legal questions"[138], and by the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés* – CNIL) stating that it allowed for broader and more intrusive surveillance measures[139], additional security laws were passed since. The 2021 law sought to codify in legislation some of the emergency powers granted to security services in the 2015 law. In addition, the law introduces also the facilitation of information exchange between security services, the extension of time during which data collected is kept, obliging telecommunication operators to exchange them with intelligence services. Despite these additional powers being granted, **the oversight mechanism still has no enforcement powers** (see section 5.6).[140]

The Code on Internal Security also defines the **type of intelligence gathering** available to these agencies. They are, inter alia:

- administrative access to connection data including:
    - delayed access to connection data; (art. L. 851-1)
    - real time access to connection data (art. L. 851-2)
    - the automated process on connection data using operators' networks or online service providers (art. L. 851-3)
    - real-time localisation (art. L. 851-4)
    - localisation using a specific device (*balisage*) (art. L. 851-5)

[135] Dambrine, B. 2015. The State of French Surveillance Law. Future of Privacy White Paper. 22 December 2015. The Law is available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899 .

[136] Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

[137] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement – Exposé des motifs.

[138] European Parliament. 2015. Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens. P8_TA(2015)0388.

[139] Opinion no 2015-078 of 5 March 2015 on intelligence bill (Délibération no2015-078 du 5 mars 2015 portant avis sur un projet de loi relative au renseignement.

[140] Ligue de Droits de l'Homme, Loi renseignement 2 : refuser l'emballement sécuritaire, June 2021, available at : https://www.ldh-france.org/loi-renseignement-2-refuser-lemballement-securitaire/

- the collection of connection data by IMSI-catcher (art. L. 851-6)

- security interception:
  - the interception of communications routed through the networks of electronic communications operators or online service providers (art. L. 852-1)
  - the interception of communications exchanged within a private network exclusively using the hertzian channel and not involving the intervention of an electronic communications operator (art. L. 852-2)
- recording of words spoken privately (article L. 853-1);
- capturing images in a private place (article L. 853-1);
- the collection or capture of computer data (article L. 853-2).

4.7. Italy

While the Italian Constitution does not expressly refer to a right to privacy or data protection, the Constitutional Court and Supreme Court regularly defined the privacy as a fundamental human right[141]. The Italian Criminal Code (Codice Penale) punishes **hacking** (i.e. the unauthorised access to IT and telematic systems - art. 615-ter)[142] of **up to three years imprisonment**. This can rise to **five years** in cases where:

1) The offence is committed by a public official or a person in charge of a public service, with abuse of powers or with violation of the duties inherent to the function or service, or by whoever exercises the profession of private investigator even illegally, or with abuse of the quality of system operator;
2) The guilty party uses violence against things or people to commit the crime, or if he is clearly armed;
3) The fact results in the destruction or damage of the system or the total or partial interruption of its operation, or the destruction or damage of the data, information or programs contained therein.

Malware, including **spyware** is criminalised by art. 615-quarter of the Codice Penale and covers anyone who "*illegally procures, holds, produces, reproduces, disseminates, imports, communicates, delivers, makes available to others or installs equipment in any other way, tools, parts of equipment or tools, codes, keywords or other means suitable for accessing a computer or telematic system, protected by security measures*".[143] This article clearly covers the **illegal import and procurement** of spyware. The crime is punished by **up to one year imprisonment and a fine of EUR 5 164**.

[141] Building on Articles 14 (inviolability of domicile) and 15 (confidentiality of correspondence), both the Constitutional Court (Dec. n. 81/1993) and the Supreme Court of Cassation (Dec. n. n. 2129/1975 - Soraya) have regularly defined the privacy as a fundamental human right.

[142] Article 615-ter Codice Penale, available at : https://www.gazzettaufficiale.it/sommario/codici/codicePenale own translation.

[143] Article 615-quarter Codice Penale, available at : https://www.gazzettaufficiale.it/sommario/codici/codicePenale own translation.

The report on hacking by law enforcement authorities published in 2017 found that **Italian law enforcement agencies use hacking tools in the process of criminal investigations**.[144] In fact, experts considered that the use of malware was the "method of choice" for Italy's law enforcement agencies.[145] Initially, Italian courts did not consider hacking-based surveillance of devices to constitute a wiretap. As such, no judge warrant was required in order to use these technique and law enforcement authorities could rely on an order from the public prosecutor. Three cases from the Supreme Court of Cassation are of particular importance:

- **Court of Cassation, 2015**[146]**:** the judgements ruled that specific conditions should be met if hacking tools are to be used for intercepting communications – e.g. the "surveillance should take place in clearly **circumscribed places**, identified at the outset, and not wherever the subject might be";[147]
- **Court of Cassation, 2016:**[148] a 2016 case referred the issue to the most authoritative session of the Court of Cassation (i.e. the 'Joint Sessions' – SS.UU.). The outcome of the 'Joint Sessions' was that the use of hacking tools is **permitted** for the interception of communications but when it is not possible for the location to be identified individually and when criminal activities have not been committed, it is **only permitted for criminal proceedings on organised crime and terrorism**. Furthermore, the decision separated the operational modes of hacking tools into two categories: 'online surveillance' and 'online search'. The former category relates to the interception of an information flow between devices (e.g. microphone, video, keyboard etc.) and the microprocessor of the target device. 'Online search' relates to copying the memory units of a computer system;[149]
- **Court of Cassation, 2018**[150]**:** a 2018 case referred to several people involved in a corruption investigation. As part of the investigation, malware was introduced into one of the defendants' mobile phones, allowing for the recording of conversations inside their home. The information collected was part of the evidence used to charge the person in question. The ruling pointed to the **need for an update** of rules and practices on hacking for surveillance purposes.[151]

Given the restrictions in the Code of Criminal Proceedings on the use of certain procedural techniques, which are prohibited when carried out at home or another privately-owned structure, unless there is a

---

144 Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016), and Citizen Lab. 2014. Mapping Hacking Team's "Untraceable" Spyware.: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

145 European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, p. 59.

146 Italian Court of Cassation, Division VI, Musumeci Case – Decision No. 27100, of 26 May 2015.

147 Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

148 Italian Court of Cassation, Joint Sessions, Scurato Case – Decision No. 1 July 2016.

149 Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. *Digital Evidence and Electronic Signature Law Review*, 13(2016).

150 Italian Court of Cassation, Decision Num. 45486, 8 March 2018, available at: http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snpen&id=./20181009/snpen@s60@a2018@n45486@tS.clean.pdf.

151 See Privacy International, Italy's Supreme Court decision limits hacking powers and applies safeguards, November 2018 available at: https://privacyinternational.org/news-analysis/2423/italys-supreme-court-decision-limits-hacking-powers-and-applies-safeguards.

reasonable suspicion that criminal activity has taken place in that location (art. 266-2), "online surveillance" could have been seen as illegal in many cases. The Supreme Court argued that given the threat posed by "*structured criminal organizations that have sophisticated technologies and significant financial resources*", online surveillance could be legal under article 266 but **required a warrant** and should be limited exclusively to proceedings relating to offences of **organized crime and terrorism** as per the jurisprudence of the Scurato case discussed above..[152]

Article 266 of the Code of Criminal procedure allows for the "*interception of conversations or communications*" in proceedings for **certain defined serious crimes**. The crimes include crimes for which the penalty is over four years' imprisonment, crimes related to drugs, weapons and explosives, as well as smuggling, pedo-pornography, selling fraudulent foods, counterfeit goods, fraud and sale of fraudulent goods, persecution, and involvement on organised crime (*associazione di tipo mafioso*). In addition, crimes using the telephone as an object are also covered.

This is extended to the "*interception of the flow of communication related to computerised systems*"(art. 266-bis).

In 2020, a new decree came into force clarifying the practices on the use of trojans to investigate crimes against the public administration committed by public officials.[153] It allows for the interception to take place at "the target's private home," even if a crime is not occurring at the moment, as long as it has been **authorized** by a judge.[154]

Italy is one of the countries examined where hacking techniques are **used directly by law enforcement authorities**. As such, the involvement of intelligence agencies is less relevant. The main intelligence agencies in Italy are:

- The **Agenzia Informazioni e Sicurezza Esterna** (AISE), focusing on foreign intelligence;
- The **Agenzia Informazioni e Sicurezza Interna** (AISI), focusing on internal security.

Both agencies **can carry out tapping activities** and preventive controls on communications 'when these are deemed essential for performing the tasks assigned to them'.[155] Since the 2007 reform of the Italian secret services (modified in 2012), both organisations are under the control of the President of the Council.[156] The procedures to follow are not expressly specified. However, preventive interception must always be granted by the judicial authority, which for intelligence services is the remit of the General Prosecutor at the Court of Appeal of Rome or the National Prosecutor in charge of mafia and terrorism for relevant cases.[157]

---

[152] Italian Supreme Court of Cassation, Joint Sessions, Scurato Case – Decision No. 26889 (1 July 2016), Pres. Canzio, Conduct of Case, under "Svolgimento del processo", para. 2 - For a detailed description of the context and legal arguments, see Privacy International's Analysis of the Italian Hacking Reform, under DDL Orlando, March 2017.

[153] Decreto-legge n. 161/2019,

[154] See Altalex, Trojan di stato, le novità della legge di conversione sul DL intercettazioni, February 2020, available at : https://www.altalex.com/documents/news/2020/02/28/trojan-di-stato-novita-intercettazioni

[155] Article 4, Legislative Decree no. 144 of 27 July 2005, Article 4, converted into Law no. 155 of 31 July 2005, available at: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133

[156] Legge 7 agosto 2012 n.133 modifiche alla legge 3 agosto 2007, n 124 concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto.

[157] FRA, Short Thematic Report, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, legal update, 2017.

The Ministry of Foreign Affairs and International Cooperation National Authority – UAMA (Unit for the Authorizations of Armament Materials) is the authority responsible for allowing the export of dual-use items.

4.8. Netherlands

The right to privacy is protected by articles 10 (general right to privacy), 11 (inviolability of one's body), and 13 (secrecy of correspondence) of the constitution. In the Netherlands, hacking is defined as 'computer intrusion" and is defined as the 'unlawful intrusion of automated systems". The crime under article 138ab of the Code of Criminal Procedure is liable to up to two years in prison and a fine of fourth category. When the instruction leads to taking control of a device or the taping of data stored or transmitted from the device, the sanction rises to four years in prison.[158] The crime covers the use of spyware (access by a technical intervention).

Unlike some of the other countries on which this report focuses, the Netherlands has a legal framework relating to the use of surveillance techniques and special investigative measures by law enforcement and intelligence agencies which has been **updated regularly** to reflect technological advances. Two specific legislative acts reflect this, the Computer Crime Act III which entered into force in 2019 and the Intelligence and Security Services Act 2017 (Wiv 2017)[159]. Civil society organisations have been very critical of both, fearing that the extended powers granted to law enforcement and intelligence agencies equate to the creation of a surveillance state.[160]

In the field of criminal justice, the special investigation techniques relevant to the Computer Crime Act III can be ordered for any offence which warrants pre-trial detention. This includes all crimes for which the prison sentence imposed is over 4 years, Further crimes include breaking and entering, squatting, hacking, wiretapping, participation in an organised criminal group, the use of recurring discriminatory or insulting language, illegal disposal of a body, paedophilia, grooming and child pornography, violation of secret, use of violence, fraud, destruction of property (and data), hijacking of ships or planes, money-laundering.[161]

The **Computer Crime Act III** aimed to strengthen the legal instruments for the investigation and prosecution of computer crime. The law, which was discussed at length in the study on "*Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*", includes wide ranging changes to the Dutch legal system in order to make it fit for purpose in the digital age.[162] The law in includes the creations of "**hacking** power", the power to make content inaccessible,

[158] Criminal Code, available at: https://wetten.overheid.nl/BWBR0001854/2022-10-01

[159] Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017, available at: https://wetten.overheid.nl/BWBR0039896/2022-05-01

[160] See for example; EDRi, Dutch Parliament: Safety net for democratic freedoms or sleepnet? , available at: https://edri.org/our-work/dutch-parliament-safety-net-democratic-freedoms-sleepnet/ or Amnesty International: Netherlands: End dangerous mass surveillance policing experiments, available at: https://www.amnesty.org/en/latest/press-release/2020/09/netherlands-end-mass-surveillance-predictive-policing/

[161] Article 67(1) of the Code of Criminal Procedure, available at: https://wetten.overheid.nl/BWBR0001903/2022-10-01#BoekEerste_TiteldeelIV_AfdelingTweede_Paragraaf1 The crimes are defined in the Criminal code, available at: https://wetten.overheid.nl/BWBR0001854/2022-10-01

[162] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

the criminalisation of gathering and offering online (stolen) data and the (extended) criminalisation of online commercial fraud and "grooming".[163]

The law explicitly **regulates** remote searches, the use of policeware, and other forms of hacking, as an investigative method, as a special investigative power. It grants Dutch law enforcement agencies the power to:

- **Remotely access/hack** electronic devices, which may or may not be connected to the internet;
- After accessing the device: **search** the device, to **activate** applications (including webcams and microphones), to **copy or delete** data.

The above is laid down in the new **Sections 126nba, 126uba and 126zpa** of the Code of Criminal Procedure.

While the clarification of the law was deemed necessary to reflect technological advances, the law has a number of shortcomings according to Bits of Freedom, a Dutch foundation, member of EDRi focusing on digital rights:[164]

- Even though the Explanatory Memorandum to the law states these investigative powers should only be used in exceptional cases, this is not stated in the law itself: the investigative powers (including turning on webcams remotely) **can be used for any criminal offence** which carries a sanction of **four years or more** (so not only terrorism and cybercrime), if it is considered to "seriously breach the rule of law";
- There is a risk that the investigative **judge** that needs to provide for the required authorisation does **not have enough knowledge** of each case for which legal hacking is requested, which carries a risk of abuse of the investigative power.

The country's intelligence services are relevant to this report, given (i) the AIVD's role in the Ridouan Taghi case[165], and (ii) the powers granted by the Intelligence and Security Services Act 2017. The two main services in the Netherlands are:

- The **General Intelligence and Security Service** (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) is the intelligence and security agency of the Netherlands, tasked with domestic, foreign and signals intelligence and protecting national security. It focusses on internal counter-intelligence and security and is under the responsibility of the ministry of the interior;
- The **Dutch Military Intelligence and Security Service** (Militaire Inlichtingen- en Veiligheidsdienst, MIVD), the military intelligence service of the Netherlands. The MIVD is under the responsibility of the Ministry of defence.

According to the Intelligence and Security Services Act 2017[166], one of the AIVD's tasks is to conduct investigations into organisations and people who pose a threat to the survival of the democratic legal order or to security or other weighty interests of the state (article 8(2)(a)). The MIVD is in charge, inter alia, of gathering information to prevent activities that harm the security or preparedness of the armed

[163] Simmons and Simmons, Pioneering Dutch Computer Crime Act III entered into force, March 2019.

[164] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.

[165] The AVID has allegedly been using Pegasus in order to help the police trace a suspect. See section 3.8.

[166] Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017), available at: https://wetten.overheid.nl/BWBR0039896/2022-05-01

forces (article 10(2)(c)(i)). In order to do so, both organisations may use techniques including (but not limited to):

- **Searching** confined places and closed objects, with or without the aid of technical aids; (article 42);
- Targeted **tapping**, receiving, recording and **eavesdropping** of any form of conversation or electronic communication, including by means of a telephone or internet tap (article 47);
- The **untargeted interception** of electronic communication, subsequently determining its nature, determining or verifying the persons or organizations involved, and finally applying automated data analysis to the metadata and selectively selecting the content data for further analysis (artides 48- 50). This is a particularly controversial part of the law, dubbed dragnet by critics [167].

In order to use these techniques, the principles of necessity, proportionality and subsidiarity must be adhered to. These techniques can only be used with the **prior approval of the Minister responsible** (article 30(1)). In cases where a **lawyer or a journalist is targeted, the additional oversight of a court is necessary, with the District court of the Hague being responsible for granting permission** (articles 30(2) and 30(3)).

The law also sets up an review mechanism, the *Toetsingscommissie inzet bevoegdheden* (TIB), in charge of reviewing the permission granted by the minister. The TIB's assessment is binding (article 32). The TIB also publishes an annual report. The effectiveness of this oversight mechanism and others is discussed in greater detail in section 5.8.

In the Netherlands, the Ministry for Foreign Affairs (Directorate-General for International Relations - Department for Trade Policy and Economic Governance) is responsible for export controls.

4.9. Other countries

United Kingdom

The legal framework for hacking by the **UK's** law enforcement agencies and intelligence services is outlined in Part 5 (Equipment Interference)[168] of the **Investigatory Powers Act** (**IPA**),[169] which came into effect in November 2016. The IPA is accompanied by six Codes of Practice that provide the corresponding operational details and judicial oversight arrangements of the powers contained within the Bill.[170] A draft Equipment Interference Code of Practice[171] (EICP) was published in August 2016 and includes legal guidance for law enforcement agencies and intelligence services wishing to conduct lawful hacking. It is important to note that the EICP and the IPA only legislate for hacking with the purpose of obtaining communications, equipment data or other information, as opposed to, for example, hacking to disrupt a system.[172] Any other forms of hacking by the national law enforcement falls under the category of 'property interference', and is governed by Part 3 of the Police Act 1997 ('the 1997 Act').[173]

---

[167] See for example Bits of Freedom, Dutch Senate votes in favour of dragnet surveillance powers, July 2017, available at: https://www.bitsoffreedom.nl/2017/07/12/dutch-senate-votes-in-favor-of-dragnet-surveillance-powers/

[168] Investigatory Powers Act 2016 (c. **25**) Part 5 – Equipment interference.

[169] Investigatory Powers Act 2016. Chapter 25.

[170] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny (2016).

[171] Equipment Interference DRAFT Code of Practice, Autumn 2016.

[172] Equipment Interference DRAFT Code of Practice, Autumn 2016, *Scope and Definitions.*

[173] Police Act 1997. C. 50 Part III Authorisation of Action in Respect of Property.

The UK does not appear to have used Pegasus or equivalent spyware. In October 2021, Princes Haya, the ex-wife of Dubai's ruler and her lawyer's phones were discovered to have been **targeted by Pegasus**. NSO subsequently claimed it had hard-coded a change preventing the targeting of UK phone numbers by the spyware.[174] This was followed by the revelation that multiple suspected instances of Pegasus spyware infections had been detected within official UK networks. These included the **Prime Minister's Office (10 Downing Street) and the Foreign and Commonwealth Office (FCO)** (Now the Foreign Commonwealth and Development office – FCDO). The suspected infections relating to the FCO were associated with the **UAE, India, Cyprus, and Jordan**. The suspected infection at the UK Prime Minister's Office was associated with a Pegasus operator linked to the **UAE**.[175]

Israel

The term 'hacking' is not a legal term in Israel and that, instead, the executing authorities use the term 'legal penetration'. This terminology legalises data collection for investigations and 'device-penetration' or hacking. Moreover, whilst computer hacking is only lawful when executed by warrant or court order and when conducted by an officer of the law during a search, there are questions about what actually constitutes lawful exercise of a hacking order.[176]

In relation to Pegasus and Israeli spyware in general, Israel claims to have acted 'in accordance with its defence export control law, complying with international export control regimes' despite **not being a participating State of the Wassenaar Arrangement**.[177] Defence exports in Israel are governed by the **Defence Export Controls Agency (DECA), a department of the Ministry of Defence**. Under the Defence Export Controls Act, DEC is the "authority for **export control**" on behalf of the Director General of the Ministry of Defence". DECA has been accused of encouraging defence and cyber companies to self-regulate and not to provide enough supervision of offensive cyber firms.[178] One reasons suggest is the close tied between many owners and managers of defence firms in Israel, who often started their careers in the Israeli Defence Forces (IDF). In addition, there have been allegations that the Israeli government had used Pegasus and similar spyware as a foreign policy tool and as a bargaining tool for the Israeli government to get support and stronger ties with third countries. As an example, *New York Times Magazine* found that countries such as **Mexico and Panama started voting in Israel's favour on some matters at the UN General Assembly after receiving the spyware**.[179]

Following the Pegasus Project revelations, and the backlisting the NSO by the USA, which effectively restricted the export of NSO product to the US or US firms, the Israeli government decided to **tighten**

---

[174] The Guardian, NSO Pegasus spyware can no longer target UK phone numbers, October 2021, available at: https://www.theguardian.com/world/2021/oct/08/nso-pegasus-spyware-can-no-longer-target-uk-phone-numbers

[175] CitizenLab, UK Government Officials Infected with Pegasus, April 2022, available at: https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/

[176] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.

[177] The Times of Israel, After NSO bombshell, Gantz asserts that Israel complies with international law, July 2021, available at: https://www.timesofisrael.com/after-nso-bombshell-gantz-asserts-that-israel-complies-with-international-law/

[178] Haaretz, Former State Watchdog Warned Israel About NSO Almost a Year Ago, August 2021, available at: https://www.haaretz.com/israel-news/2021-08-06/ty-article/.premium/former-comptroller-warned-israel-about-nso-activities-almost-a-year-ago/0000017f-df04-df9c-a17f-ff1c76e20000

[179] See Haartez, The Pegasus Project | Where Netanyahu Went, NSO Followed: How Israel Pushed Cyberweapon Sales, July 2021, available at: https://www.haaretz.com/israel-news/tech-news/2021-07-20/ty-article/.highlight/where-bibi-went-nso-followed-how-israel-pushed-cyberweapons-sales/0000017f-e388-d7b2-a77f-e38fd45a0000

Council of Foreign Relations, How Israel's Pegasus Spyware Stoked the Surveillance Debate, March 2021, available at: https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate

the control of cyber exports. The move changed the end user declaration that buyers must sign to refine and tighten the definition of terrorism which was arguably previously used in a very broad sense[180]. In addition, the country **reduced the list of countries eligible to exports of defence cyber technologies to 37, from an initial 102**[181].

USA

The **FBI has admitted purchasing the Pegasus spyware**. However, it claims to only have purchased a limited license for testing and evaluation in order to assess the harm the spyware could do if use maliciously.[182] In addition, **State Department employees in Uganda have been targeted** by the spyware.[183]

There is no detailed piece of US legislation specifically regulating the use of hacking by law enforcement.[184] Whilst federal statutes such as Part I of the Electronic Communications Act (ECPA) (1986)[185] – an expansion of the 'Wiretap Act' (1968)[186] – and the Stored Communications Act (SCA)[187] govern law enforcement surveillance of real-time and stored communications respectively, both statutes pre-date the use of government hacking.[188] Instead, although never expressing it as absolute policy,[189] law enforcement agencies have generally sought authorisation for the use of hacking in investigations in search and seizure warrants applied under Rule 41 of the Federal Rules of Criminal Procedure (Rule 41).[190] The amendments to Rule 41 in December 2016[191] appear to confirm it as the most relevant piece of US legislation by offering a procedure for law enforcement agencies to gain 'remote access' of data.[192]

As a result of the revelations from the Pegasus project, the US Commerce Department's Bureau of Industry and Security (BIS) announced a rule to prevent the distribution of surveillance tools, like NSO Group's Pegasus, to countries subject to arms controls.[193] In terms of imports, **NSO Group and Candiru**

---

[180] Israeli Ministry of Foreign Affairs, Israel MoD tightens control of cyber exports, December 2021, available at: https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021

[181] The Times of Israel, Amid NSO scandal, Israel said to ban cyber tech sales to 65 countries, November 2021, available at: https://www.timesofisrael.com/amid-nso-scandal-israel-said-to-ban-cyber-tech-sales-to-65-countries/

[182] The Guardian, FBI confirms it obtained NSO's Pegasus spyware, February 2022, available at: https://www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware

[183] Reuters, U.S. State Department phones hacked with Israeli company spyware – sources, December 2021, available at: https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/

[184] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.

[185] 18 U.S.C. § 2510 – an expansion of the Wiretap Act to include digital communications

[186] Omnibus Crime Control and Safe Streets Act (1968), P.L. 90-351, 801, 82 Stat. 197, 212 – provides the US government with procedural regulations surrounding the interception of real-time telecommunications.

[187] 18 U.S.C. Chapter 121 §§ 2701–2712

[188] The first report of the US government possessing the capability to use remote hacking in an investigation was in 2001 – Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Background on Amendment to Rule 41.

[189] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017

[190] Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service

[191] FED. R. CRIM. P. 41.

[192] FED. R. CRIM. P. 41. (b) (6)

[193] The Register, Uncle Sam to clip wings of Pegasus-like spyware – sorry, 'intrusion software' – with proposed export controls, October 201, available at: https://www.theregister.com/2021/10/20/us_intrusion_software_rules/

(Israel) were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers.[194]

[194] US Department of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, November 2021, available at: https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

5. OVERSIGHT AND REDRESS

This chapter focuses on the democratic and judicial oversight mechanisms in place in the countries covered by this report. It describes the ex-ante and ex post judicial and democratic oversight; and redress mechanisms in case of illegal use of spyware.

In a democratic society, law enforcement and intelligence services shall strive to operate effectively while fully complying with democratic norms and standards, rule of law requirements and fundamental rights. They shall be politically neutral and non-partisan, adhere to a strict professional ethic and operate within their legal mandates, in accordance with the constitutional-legal norms and democratic practices of the state. Public accountability is necessary to eliminate any risk of abuse of power. While this seems to be the case for law enforcement authorities like the police, that normally operate on the basis of judicial authorisations and are subject to judicial review, parliamentary oversight and judicial control of intelligence services present unique difficulties given the need for them to maintain the highest level of secrecy. In a democratic state, intelligence services should strive to be effective.[195]

5.1. Greece

5.1.1. Ex-ante – oversight

In order to use special investigative techniques in criminal cases, law enforcement authorities must seek the authorisation of the public prosecutor who submits a request to the judicial council. The decision can only be granted if it involves the investigation of a criminal act, there is serious suspicion of guilt against the person targeted, there are no alternatives to the measure, and the use of technique is limited in time. In urgent cases, the public prosecutor may allow the use of the technique before referring to the judicial council. The request must be submitted to the judicial council within three days, alongside the reasoning for the urgency of the decision. If the judicial council rules against the validity of the request the information collect cannot be used in court.[196]

For intelligence services, the process is similar. In order to fulfil its mission, the EYP has access to special investigative techniques, including the lifting of confidentiality of communication, recording the activities of individuals using special technical media, especially audio-visual devices, outside residences.[197] There are ex-ante mechanisms to ensure this is done in a legal way.

In order for the EYP to be able to use these techniques, a **judicial order** must have been issued by the **Public Prosecutor of the Court of Appeal**, specially **assigned to the EYP**, who supervises the EYP and controls the legality of its special operational activities as set out in art. 5 of Law 3649/2008.

Once the order is granted, a **copy** must be handed to the president, administrative council, general director or representative of the legal entity responsible for waiving confidentiality (in case where a

[195] Gill, Peter. 2003. Democratic and Parliamentary Accountability of Intelligence Services after September 11th. Geneva, January 2003. Geneva Centre for the Democratic Control of the Armed Forces. Working Paper No. 103, quoted in Geneva Centre for the Democratic Control of Armed Forces, Intelligence practice and democratic oversight – a practitioner's view, July 2003

[196] Article 154 (3) of the Code of Criminal Procedure, available at: https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4620-2019/arthro-254-kodikas-poinikis-dikonomias-nomos-4620-2019

[197] Law 3649/2008, article 5

telecommunications company is involved) , as well as to the Hellenic Authority for Communication Security and Privacy (ADAE).[198]

Once the approval has been granted, one or more reports are prepared by the responsible service and are submitted to the judicial authority that issued the order, as well as to ADAE and the applicant authority (see Article 5(5) of Law 2225/1994). According to law, the measures cannot exceed **10 months** (except when done for reasons of national security).

In December 2022, the new law on Communications de-privacy process, cyber security and protection of citizens' personal data approved by the parliament provides additional safeguards. The speaker of the parliament must approve the monitoring of politicians' phones. Furthermore, the target must be informed three years after the surveillance has taken place if the prosecutor allows it.[199]

The **lack of effective ex-ante mechanisms** is also the result of **conflict of interests** which have emerged since the uncovering of the use of predator in Greece. The General Secretary of the Prime Minister, Grigoris Dimitriadis, had ties to the software company that distributes the Predator software in Greece. This one of the reasons Mr Dimitriadis resigned alongside the president of the EYP, Panagiotis Kontoleon.[200]

The **lack of identification of a problem** through the ex-ante mechanisms in place tend to show the lack of effectiveness of these mechanisms. The cases of the journalists and politicians whose phones have been infected by Predator were uncovered by CitizenLab, after the journalists approached them, fearing that they had been hacked. Without the work of investigative journalists, civil society, and investigative insight from pressure from bodies such as the European Parliament, breaches of law and privacy would have continued despite the existing ex-ante oversight mechanisms.

5.1.2. Ex-post – sanctions and remedies

In terms of ex-post oversight mechanisms, the Greek legal order establishes **some safeguards** relating to the use of spyware. First of all, the Greek **constitution** enshrines the right to be "protected from the collection, processing and use, especially by electronic means, of their personal data" (art. 9A)[201]. In addition, the Hellenic Data Protection Authority (HDPA) is competent for investigating cybercrimes that involve the processing of personal data. Greek law stipulates the right to access information on whether a person is the object of a surveillance scheme (Law 2472/1997)[202]

After the initial revelation of the use of Predator in Greece, the government controversially adopted an amendment (as part of the law addressing COVID-19 emergency measures). This amendment removed the right for targets of monitoring to be informed, even after the end of the monitoring period, if this

---

198 FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, Greece, October 2014, p. 18.

199 See the draft law available at: https://www.hellenicparliament.gr/Nomothetiko-Ergo/Katatethenta-Nomosxedia?law_id=3715dd48-9b39-4532-9b0e-af5c014ff48e

200 PEGA committee, hearing on Use of Spyware in Greece 8 September, 8 September 2022, available at: https://emeeting.europarl.europa.eu/emeeting/committee/en/agenda/202209/PEGA?meeting=PEGA-2022-0908_1&session=09-08-09-00

201 The Constitution of Greece, revised by Resolution of November 25, 2019 of the IXth Revisionary Parliament, English translation provided by the Hellenic Parliament, available at: https://www.hellenicparliament.gr/en/Vouli-ton-Ellinon/To-Politevma/Syntagma/

202 Law 2472/1997 'On the protection of individuals with regard to the processing of personal data (as amended)*('Για την προστασία των δεδομένων προσωπικού χαρακτήρα')*, (O.G. A΄ 50/ 1997). An English version is available at : https://www.dpa.gr/sites/default/files/2019-10/law_2472-97-nov2013-en.pdf

is motivated by national security reasons.[203] This change allows those conducting monitoring activities to carry them out in the knowledge that they have no legal obligation to disclose this information in the future, hereby removing an important procedural guarantee.

There are three main relevant **oversight** bodies and related mechanisms in the country:

- The **Authority for Communication Security and Privacy (ADAE)** – which is non-parliamentary committee designated by Parliament and appointed by the Minister of Justice, Transparency and Human Rights overseeing the EYP, the Hellenic police and the State Security Division. ADAE has the competence to oversee telecommunication agencies, but not public services nor general private organisations, as its mandate only allows it to control networks of providers and conduct technical controls. ADAE can issue regulations regarding the assurance of the confidentiality of communications, perform audits on communications network/service providers, public entities, as well as the EYP, and hold hearings, investigate complaints and collect relevant information using special investigative powers Finally, ADAE has the obligation to inform the targets of investigations breaching the confidentiality of communication , provided that the purpose of the investigation is not compromised;[204]
- The **Hellenic Data Protection Authority** (HDPA). An independent Authority not subjected to any administrative control. It pertains and answers to the Minister of Justice for budgetary purposes. The HDPA proceeds ex officio or following a complaint to administrative reviews in the framework of which the technological infrastructure and other means, automated or not, supporting the processing of data are reviewed. It has the power to examine complaints and to report violations in the field of the protection of personal data;
- The **Special Standing Committee for Institutions and Transparency** – a parliamentary committee in charge of overseeing policies; administration and management; and the legitimacy of the activities of the EYP. The committee oversees the National Intelligence Service.

Remedies through **legal means** are also possible. Thanasis Koukakis, one of the targets of the EYP, has filed a **lawsuit** against Intellexa, the company responsible for the development of Predator and its owners. The lawsuit includes accusations of breaches of privacy and communications laws. One of the reasons for this is the fact that despite revelations on the use of Predator, Intellexa has not been prevented from trading in the country.[205] The case is still pending.

Following the change of the law on surveillance, a conflict has arisen between the Supreme Court Prosecutor and ADAE on the powers of the latter to inquiry on citizens' complaints.[206]

---

[203] Inside Story, Violation of the legislative process for amendments in law 4790/2021, March 2021, available at: https://insidestory.gr/article/who-was-tracking-mobile-phone-journalist-thanasis-koukakis
https://govwatch.gr/en/finds/violation-of-the-legislative-process-for-amendments-in-law-4790-2021/

[204] FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, Greece, October 2014, and EP PEG committee Hearing on 'Use of spyware in Greece', see: https://www.europarl.europa.eu/committees/en/pega-hearing-on-use-of-spyware-in-greece/product-details/20220912CHE10601.

[205] Haaretz, Criminal Allegations Against Israeli-linked Spyware, Ex-intel Commander in Greek Hacking Scandal, October 2022, available at: https://www.haaretz.com/israel-news/security-aviation/2022-10-07/ty-article/.premium/criminal-allegations-against-israeli-linked-spyware-ex-intel-commander-in-hacking-scandal/00000183-ad14-d3f8-a9ef-bf5752e60000

[206] https://www.euractiv.com/section/politics/news/chief-prosecutor-puts-greeces-rule-of-law-to-the-test/

5.2. Spain

5.2.1. Ex-ante – oversight

In the field of criminal cases, the Judiciary Police or the Public Prosecution Services must ask authorisation to use special investigative techniques. A judge is responsible for allowing the use of the investigation technique (including the use of spyware). In order for an order to be granted, it must include inter alia:

- The description of the event under investigation,
- A detailed justification of the grounds for the use of the technique,
- The extent of the measure and specification of its content,
- The duration of the measure applied for.[207]

The judge has 24 hours to respond to the request. Once granted, the measure has to be limited in time, the Judiciary Police must inform the magistrate about the development and the use of the technique.[208]

In terms of surveillance by intelligence services, the process is different. The ex-ante oversight mechanisms for the CNI (which was responsible for the use of spyware in Spain) are set out in Organic Law 2/2002, which prescribes a special procedure to request judicial authorisation for surveillance activities, and Law 11/2002 which establishes parliamentary control by the Official Secrets Committee of the Spanish Congress. The CNI is under the executive control of the Delegated Committee for Intelligence Affairs which coordinates its intelligence-related activities. Parliamentary oversight is exercised by the Defence Committee of the Congress of Deputies.[209]

The **CNI can ask a Magistrate of the Supreme Court for authorisation to intercept** communications on the grounds of a threat to the territorial integrity of Spain or the stability of the rule of law "provided that such measures are necessary for the fulfilment of the tasks assigned to the Centre"[210]. The authorisation can be based on much looser concepts, which, in the words of a professor of constitutional law, "almost anything can fit".[211]

Following the revelations of the CNI's use of Pegasus and Candiru, Spain' **Ombudsperson**, the *Defensor del Pueblo* was tasked with investigating the legality of the practice. The investigation concluded that: "the CNI took action respecting the various legal provisions for prior judicial control of the intervention in communications that took place in the cases of a part (18) of the people alluded to in different media information published in April".[212]

---

[207] Art 588 a. ii. of the Criminal Procedural Code.

[208] Art 588 a. iii. to 588 a. xi. of the Criminal Procedural Code.

[209] Florina Cristiana Matei, Andrés de Castro García & Carolyn C. Halladay (2018), On Balance: Intelligence Democratization in Post-Franco Spain, International Journal of Intelligence and CounterIntelligence, 31:4, 769-804, DOI: 10.1080/08850607.2018.1466588 p.776, available at: https://doi.org/10.1080/08850607.2018.1466588

[210] Law 2/2002, 6 May, Regulating The Prior Judicial Control Of The National Intelligence Center (Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.), available in English at: https://www.global-regulation.com/translation/spain/1451142/law-2-2002%252c-6-may%252c-regulating-the-prior-judicial-control-of-the-national-intelligence-center.html

[211] EPRS, Europe's PegasusGate – countering spyware abuse, July 2022.

[212] Defensor del Pueblo, El Defensor del Pueblo verifica que la actuación del CNI se ha realizado conforme a la Constitución y la Ley en los casos examinados, May 2022 ? available at : https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/

CitizenLab's conclusion on the role of the government, raised "*urgent questions about whether there is proper oversight over the country's intelligence and security agencies, as well as whether there is a robust legal framework that authorities are required to follow in undertaking any hacking activities*".[213]

In May 2022, after the story broke, the government announced two initiatives. The first one is to **update the law on official secrets**, which dates from 1968, and had not been revised since the country's transition to democracy. The second is a **revision** of the Organic Law Regulating Prior **Judicial Control of the CNI** with the aim to strengthen the guarantees of this control, as well as to ensure maximum respect for individuals' political and individual rights.[214]

The public consultation for the update of the law on official secrets was initiated in August 2022 and its contents were criticised by civil society organisations, as well as the fact that holding the consultation in August discouraged citizens' participation.[215]

5.2.2. Ex-post – sanctions and remedies

Information related to intelligence services and their activities is excluded from the law on Transparency and Access to Public Information and Good Governance.[216]

Ex-post mechanisms in Spain are principally under the auspices of:

- Spain's **Ombudsperson**, the ***Defensor del Pueblo***. As mentioned above, the *Defensor* can undertake inquiries on topics related to gathering intelligence by law enforcement authorities. It may ask the public authorities all documents deemed necessary for the development of its function, including those classified with the nature of secrets in accordance with the law. It must be noted that the *Defensor* treats complaints by individuals in relation to activities conducted by the police but not by the CNI;
- **Official Secrets Committee** of the Spanish Congress (officially the Commission for the Control of Credits Allocated to Reserved Expenditures)[217]. The Committee was created in 1995.[218] The law setting up the CNI mentions that the Committee has access to classified matters. The CNI must have appropriate information on the running and activities of intelligence objectives assigned by the Government, with an annual activity report. However, by the time the committee convened in light of the Pegasus and Candiru scandals, this was its first sitting in over two years.

The fact that the *Defensor* has only been able to focus its investigation on 18 people which were targeted by spyware following a court authorisation and to conclude on the lack of breach of the legal framework in those cases demonstrates that this ex-post oversight mechanism is not as effective as it

---

213 Citizen Lab, CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru, April 2022, available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

214 La Moncola, president's news, Pedro Sánchez announces a reform of the legal control regulation of the National Intelligence Centre (CNI) to strengthen its guarantees, May 2022, available at: https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx

215 See Access Info, Alegaciones al Anteproyecto de la Ley de Información Clasificada, August 2022, available at: https://www.access-info.org/wp-content/uploads/2022-08-12-Access-Info-Alegaciones-Ley-de-Informacion-Clasificada.pdf

216 Law 19/2013 on Transparency, Access to Public Information and Good Governance (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno).

217 Comisión de control de los créditos destinados a gastos reservados, usually called Comisión de Secretos Oficiales.

218 Law 11/1995, of May 11, regulating the use and control of credits for reserved expenses Ley 11/1995, de 11 de mayo, reguladora de la utilización y control de los créditos destinados a gastos reservados, available at: https://www.boe.es/buscar/act.php?id=BOE-A-1995-11339

could be. The same can be said about the parliamentary commission, given it had not convened in over two years at the time when a scandal was unfolding.

From a judicial point of view, there are no specialised judges appointed for surveillance cases in Spain[219]. Anyone has the right to obtain effective protection of the Judges and the Courts in the exercise their legitimate rights and interests. In this sense, any citizen considering their fundamental rights have been violated can seek **judicial redress**.

Targets of the Pegasus and Candiru spyware from the CNI have **filed a lawsuit** in Spain, as well as in the countries where the targets were located when spied upon. The lawsuit is **against NSO, one of its subsidiaries, and its three founders, but not against the Spanish state**.[220] The case is still pending.

5.3. Hungary

5.3.1. Ex-ante – oversight

The right to privacy and the protection of personal data is enshrined in the **Fundamental law** (para. 1 and 2). Like all other Member States, Hungary has also ratified the International Covenant on Civil and Political Rights (ICCPR), the ECHR and is bound to the Charter of Fundamental Rights of the EU, which all contain provisions on privacy and the protection of personal data.

Law Enforcement Authorities can make use of special investigative techniques (also referred to as covert instruments in the code of criminal procedure), including covert surveillance of information systems and wire-tapping. These instruments may be used if there is a reasonable suspicion against a defendant. The use of covert instruments may be applied by the prosecutor's office and the investigating authority and approved by a judge designated by the Budapest Metropolitan Court.[221] With regards the use of surveillance measures by intelligence services, National Security Act provides **limited oversight** on surveillance measures by the police or intelligence agencies. The ex-ante oversight mechanisms set out in the National Security Act include:

- The **prior authorisation** needed to be provided by:
    - the **Minister of Justice** for intelligence information gathering by all National Security Services[222]
    - The **Metropolitan Court of Budapest** in certain 'exceptional' cases (which are not specified)[223]
- The **Parliamentary Committee on National Security** (*Országgyűlés Nemzetbiztonsági Bizottsága*).[224] In exercising parliamentary supervision, the Committee is entitled to request information from the Minister and the directors of the national security services about the country's national security situation and the functioning and activities of the services.

In order to obtain authorisation for the use of special investigation techniques by the intelligence services, a **request** has to be submitted by the relevant services of the intelligence agency to the

[219] Article 24 of the Spanish Constitution

[220] Mediapart, Pegasus : vers un nouveau front judiciaire pour les indépendantistes catalans, April 2022, available at : https://www.mediapart.fr/journal/international/250422/pegasus-vers-un-nouveau-front-judiciaire-pour-les-independantistes-catalans

[221] Code of Criminal Procedure, articles 231-242, available at: https://net.jogtar.hu/jogszabaly?docid=a1700090.tv

[222] Act CXXV of 1995 on the National Security Services, Article 58(2).

[223] Act CXXV of 1995 on the National Security Services, Article 58(1).

[224] Act CXXV of 1995 on the National Security Services, Article 14.

general director of the relevant agency. The demand must include (i) the location, (ii) the person or group of people concerned, (iii) justification for the necessity of the intelligence gathering, (iv) start and end date of the gathering activity. The Minister of justice then has 72 hours to make a decision. This decision cannot be appealed.

Intelligence gathering can be authorised for a maximum of **90 days**, which can be extended by a further 90 days. The intelligence information gathering shall be terminated under three conditions: (i) it has achieved its objectives, (ii) no results can be expected if it continues, and (iii) it is found to be unlawful in any respect.[225] However, given the secrecy of these services, the rules are not available to the public.

The type of crimes or the criteria needed to warrant the use of special investigative techniques by intelligence agencies are not set out clearly in the National Security Act.

The **ex-ante oversight mechanisms appear ineffective in the context of surveillance**. In light of the *Szabó and Vissy* ECtHR judgment, the National Authority for Data Protection had proposed amendments to the law which would have clarified the conditions under which the state could conduct covert surveillance and allowed for an independent body to be involved in the authorisation process,[226] but these were rejected by the government. The government's refusal to amend the legal framework to strengthen the ex-ante oversight of State surveillance through the Hungarian secret services has created the conditions for the indiscriminate use of Pegasus in the country, as reported by NGOs, media and companies.[227]

5.3.2. Ex-post – sanctions and remedies

Ex-post mechanisms are set out in the National Security Act. Anyone who becomes aware or suspects unlawful conduct from the secret services can **lodge a complaint with the Minister in charge of service concerned.** The Minister is in charge of investigating the complaint within 30 days, which can be extended by another 30 days[228]. If the plaintiff does not agree with the outcome, they can begin their **complaint to the National Security Committee** of the Hungarian Parliament, although the committee does not rule on legal grounds.

Another route is to turn to the **Ombudsperson** (the Commissioner for Fundamental Rights). Given being targeted by Pegasus or similar spyware is an attack on a person's fundamental rights, in particular article 8 ECHR, the Commissioner will investigate on the complaints received. As a first step, the Commissioner will ask the competent bodies (i.e., the Ministries overseeing the security services) to remedy any infringement. If this is no done, the Ombudsperson has the power to initiate criminal proceedings. If the issue relates to the protection of personal data, the matter can be referred to the National Authority for Data Protection and Freedom of Information (NAIH).

---

[225] Act CXXV of 1995 on the National Security Services, Article 60 (1).

[226] Hungarian Civil Liberties Union (HCLU), Communication under Rule 9.2 of the Rules of the Committee of Ministers regarding the supervision of the execution of judgments and terms of friendly settlements by the Hungarian Civil Liberties Union, January 2022.

[227] Hungarian Civil Liberties Union (HCLU), Communication under Rule 9.2 of the Rules of the Committee of Ministers regarding the supervision of the execution of judgments and terms of friendly settlements by the Hungarian Civil Liberties Union, January 2022, p.9.

[228] FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, Hungary (2014)- para 11.

The **Hungarian National Authority for Data Protection and Freedom of Information** (NAIH) is Hungary's Data Protection Authority can undertake wide-reaching investigations. Its decisions are not binding and therefore only have the power of **recommendation**.[229]

Judicial review is also available. In practice, **six of the people targeted by Pegasus** in Hungary, represented by the Hungarian Civil Liberties Union (HCLU) have **initiated proceedings**. The proceedings help shed light on the difficulties for victims to seek remedies. The HCLU underlined the limited possibilities to obtain redress in the country. The proceedings initiated are against the Constitutional Protection Office (CPO) under the Ministry of the Interior and the Information Office (IO) under the Ministry of Foreign Affairs and Trade, targeting the use and purchase of Pegasus.[230]

Shortly before that, the **Hungarian Data Protection Agency's report on the use of Pegasus** in Hungary was published. The NAIH found that in all the cases if looked into (over a hundred), **the use of Pegasus was legal** as all cases the agency investigated were done in order to avoid a threat to national security.[231] These findings cast a **question mark on the independence of the authority**, especially given the reasoning for the authority's decision is classified and will remain so until 2050.[232]

The **shortcomings** identified by the ECtHR's *Szabó and Vissy* judgment are still ongoing and have not been addressed. The existing oversight mechanisms can therefore only be deemed inadequate, and the 2016 judgment "*the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it*" can be deemed to still be valid. ,[233]

5.4. Poland

5.4.1. Ex-ante – oversight

In the field of criminal investigations, wiretapping can be used (as discussed above in section 4.4). The investigative authority (the police) must request authorisation for the use of special investigation techniques. The local district court is responsible for granting this authorisation. However, the district court judge only has access to information provided by the investigative authority.[234] As such, the information available to the judge may be sparse.

In the field of ex-ante oversight for intelligence services, **Poland has not established one single body for oversight**. At present, **the oversight of security services in Poland is fragmented**. It is exercised by the authorities of the state, such as[235]:

- **The Sejm (lower chamber of the Parliament), the Sejm Committee on Security Services, and the Senate's Special Committee** – – as part of its supervision over the activities of government administration bodies, the Sejm exercises oversight of the security services. However, the Sejm

[229] HCLU, Pegasus case: Hungarian procedures, available at: https://hclu.hu/en/pegasus-case-hungarian-procedures

[230] HCLU, Pegasus case: Hungarian procedures, available at: https://hclu.hu/en/pegasus-case-hungarian-procedures

[231] Netzpolitik, Pegasus scandal in Hungary: „Not surprising, but still shameful", February 2022, available at: https://netzpolitik.org/2022/pegasus-scandal-in-hungary-not-surprising-but-still-shameful/

[232] See Balkan Insight: Data Dealing: Oversight Concerns in Hungary over AI Data https://balkaninsight.com/2022/01/25/data-dealing-oversight-concerns-in-hungary-over-ai-data/

[233] Hungarian Civil Liberties Union (HCLU), Communication under Rule 9.2 of the Rules of the Committee of Ministers regarding the supervision of the execution of judgments and terms of friendly settlements by the Hungarian Civil Liberties Union, January 2022, p.11.

[234] Act of 15 January 2016 Amending the Police Act and Certain Other Acts, Art 20c.

[235] Bodnar, Adam et. al. (2019): How to saddle Pegasus: Observance of civil rights in the activities of security services: objectives of the reform, p. 7.

Committee on Security Services is a body composed of politicians representing individual parliamentary groups. At present, the ruling coalition has a significant majority of seats on the Committee, which significantly limits the possibilities of independent oversight. The Senate's special committee (set up in January 2022) undertook a review of the use of Pegasus in Poland, but key ministers refused to appear in front of the committee, which was possible given the committee does not have investigative powers;[236]

- **Supreme Audit Office** – exercises oversight of the services within the scope of responsibilities of the Office. The Office identified an invoice for PLN 25 million covering the purchase of Pegasus for the Central Anticorruption Bureau. It notified the irregularities it found to the Ministry of Justice, which has not followed up on this information;[237]
- **Commissioner for Human Rights (CHR)** – the country's ombudsperson exercises control over individual activities of the services, based on lodged complaints regarding the respect of civil rights;
- **State government bodies (Prime Minister, Minister** – Coordinator of Security Services, Government Council on Security Services) coordinate and control daily work of security services;
- **Courts and prosecutors** – supervise the conduct of secret surveillance and other surveillance operations by security services.
- **The Internal Oversight Bureau of the Ministry of the Interior and Administration** supervises the secret surveillance operations carried out by the Police, the Border Guards and the State Protection Service (in charge of the protection of Polish and oversees officials);
- **The President of the Polish Personal Data Protection Office** – the country's independent data protection authority.

According to a report by a group of experts who have been observing the work of security services in Poland and related risks that are emerging to the protection of civil rights and freedoms, this fragmentation of oversight **does not enable an effective, impartial and non-political verification of the activities of security services**[238].

The **lack of an independent body for oversight of security services has been highlighted and criticised** for several years by different organisations, including in a **Judgement K23/11 of the Polish Constitutional Tribunal**, which determined that the existing legal provisions – contained within the **Polish Act on Police of 6 April 1990**[239] – were insufficient and recommended a range of key amendments, to be implemented within 18 months of the decision (i.e., by 7 February 2016).[240]

[236] PEGA committee Mission report following the delegation to Warsaw, Poland 19 – 21 September 2022, available at: https://www.europarl.europa.eu/doceo/document/PEGA-CR-736647_EN.pdf

[237] Ibid.

[238] How to saddle Pegasus: Observance of civil rights in the activities of security services: objectives of the reform, p. 7

[239] Polish Act on the Police of 6 April 1990.

[240] Id.; see Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016 for a summary, pp. 5-6.

Among these recommendations was that an independent oversight body should be established, that individuals subject to surveillance be notified, and that procedural safeguards for secret surveillance be tightened[241].

To implement this judgment, the ruling Law and Justice Party implemented two Acts to regulate various methods of secret surveillance employed by law-enforcement and intelligence agencies: (1) The Act of 15th January 2016 on the **Amendment to the Police Act and other acts** (including the Act on the Internal Security Agency and Intelligence Agency); and (2) the Act of 10th June 2016 **on anti-terrorist activities**[242], which stipulates the powers of the Internal Security Agency (ISA), Poland's domestic intelligence agency.

However, **neither Act created an independent oversight body** as envisioned by the Constitutional Tribunal. Furthermore, the Police Act 2016 has been widely criticised – most notably by the Council of Europe's Venice Commission – for **expanding police surveillance prerogatives**, especially through Article 19 of the Act. Under Article 19 of the Police Act, secret surveillance is to be performed with the prior consent of a district court. As an **exception**, in cases of utmost urgency, police may perform surveillance without such prior consent; however, if consent is not granted within 5 days, surveillance must be suspended, and the material gained from it must be destroyed. However, **during these 5 days, surveillance activities are possible**[243].

Importantly, the Act does not foresee the possibility for the judge issuing the surveillance warrant to access the materials obtained as a result of surveillance. This only happens in the cases of prolongation of the wiretapping warrant, or in the cases of retroactive authorisation of the "urgent" surveillance which has been ordered without pre-authorisation. Thus, **judges have no tools to realistically check whether the services are abusing their powers**.[244]

Following the introduction of the Act of 15 January 2016 amending the Police Act and certain other acts, the Council of Europe's Parliamentary Assembly's Monitoring Committee requested the opinion of the Venice Commission. The Monitoring Committee's chair had concerns about the right to privacy implications of the law. The Venice Commission submitted an opinion on the law in June 2016. While pointing out that judicial authorisation of surveillance constitutes an important safeguard against abuse, the **Venice Commission** pointed out the risk of the overburdening of judges with such requests. In addition, judges should have appropriate assistance by staff members who have adequate insight into the technology and practice of surveillance operations, as otherwise they would tend to minimise the effort and limit themselves to a purely formal review[245]. Furthermore, the Venice Commission stressed that in the absence of a real adversarial debate, judges tend to be less critical to the position of the police, which could make the prior judicial authorisation of the surveillance measures become a simple **formality**.[246] Finally, the Commission welcomed the Act's provision that a prosecutor should

[241] Grabowska-Moroz, Barbara, 'The Polish surveillance regime before the ECHR' (about: intel, 27 April 2020); https://aboutintel.eu/echr-poland-surveillance

[242] Polish Act of 10 June 2016 on anti-terrorist activities and on the amendments to other acts. Unofficial translation available at: http://www.legislationline.org/topics/country/10/topic/5.

[243] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.

[244] Walker, Shaun, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', The Guardian, 24 January 2022, available at: https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony

[245] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 24

[246] Ibid.

participate in the process of authorisation of surveillance, but pointed out the close relations between the prosecution service and the police in the Polish system, stating that the involvement of the prosecutor cannot be considered as a sufficient procedural safeguard[247].

The **Anti-Terrorism Act 2016** was similarly criticised by Poland's Human Rights Ombudsman,[248] as well as by the Panoptykon Foundation[249]. The Act **broadens the competences of the Internal Security Agency**. In addition, the law entitles the Chief of the Internal Security Agency to order 3-months wiretapping of a foreigner, without a judicial order, if there is a risk that he/she is involved in terrorist activities[250]. It also states that the Minister of Internal Affairs defines a catalogue of situations that might be considered as "terrorist events" (*katalog incydentów o charakterze terrorystycznym*)[251]. The competences of the Internal Security Agency were also broadened to create wide access to all public registers.

5.4.2. Ex-post – sanctions and remedies

Regarding ex-post oversight of surveillance operations, the **Minister of Interior has to present to the Polish Parliament a report** on the surveillance activities carried out by the police on an annual basis. However, Art. 19 of the Police Act stipulates that the Minister's role is to give a general overview of the surveillance activities rather than justifying the necessity of specific operations.

There is no independent body that oversees specific surveillance operations, has an insight into the practice of surveillance and interception and is not institutionally linked to the police, the executive, the law-enforcement or intelligence services.

In recent years, international standards regarding the observance of civil rights in the context of the activities of security services have been developing. However, in Poland there is a **lack of a legal requirement to notify individuals that they are the target of surveillance**. One example is the Police Act, which does not contain any requirement to notify the target, even after a lapse of time. Thus, there is no provision of remedy for individuals who have been target of surveillance.

In its report, the **Venice Commission** stressed the importance to set in the Act a general obligation of the relevant authorities to **notify the target ex-post** and formulate exceptions from this rule[252]. For the time being, however, given that most targets are never notified that they are under surveillance, they are **unable to enforce their constitutional rights before Poland's courts**. In addition, the Polish law fails to meet the standards applicable to the use of wiretapping and secret surveillance, that arise from the case law of the ECtHR including the right for a target to be informed of the proceedings, the adequate and effective guarantees against arbitrariness and the existence of effective safeguards and remedies.[253].

---

[247] Ibid.

[248] Ombudsman, 'Apel RPO do Prezydenta w sprawie ustawy antyterrorystycznej' (21 June 2016) https://www.rpo.gov.pl/pl/content/apel-rpo-do-prezydenta-wsprawie-ustawy-antyterrorystycznej .

[249] Panoptykon Foundation' 'Poland adopted controversial anti-terrorism law' (22 June 2016); https://en.panoptykon.org/articles/poland-adoptedcontroversial-anti-terrorism-law .

[250] Poland, Act on anti-terrorist actions (Ustawa o działaniach antyterrorystycznych), 10 June 2016, Article 9.

[251] Poland, Act on anti-terrorist actions (Ustawa o działaniach antyterrorystycznych), 10 June 2016, Article 5.2

[252] Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016, p. 26.

[253] Klass and others v. Germany, judgment of the European Court of Human Rights of 6 September 1978, complaint No. 5029/71, Iordache v. Moldova, judgment of the European Court of Human Rights of 10 February 2009, complaint No. 25198/02, Liberty and others v. the United Kingdom, judgment of the European Court of Human Rights of 1 July 2007,

The Police Act also states that a **person subject to surveillance shall not have access to information gathered during the operational control**.[254] Such provision was not included in the Act on the Internal Security Agency and Intelligence Agency, but it is interpreted in a similar way. According to Article 27.15 of the Act on Internal Security Agency and Intelligence Agency, after conducting "operational control," the Agency shall transfer gathered material to the prosecutor's office if there is evidence of committing a crime.[255]

5.5. Germany

5.5.1. Ex-ante – oversight

In Germany, the legal framework includes some ex-ante oversight provisions for criminal cases,, namely in the **Code of Criminal Procedure** (*Strafprozeßordnung – StPO*), and the **Federal Criminal Police Office Act** (*Bundeskriminalamtsgesetz – BKAG*).

The StPO requires a range of *ex-ante* conditions to ensure practices are lawful, taking fundamental rights into account, and that data collected are admissible as evidence in court.

The Federal Criminal Police Office (BKA) may only use technical means to intervene in the information technology systems used by suspects and collect data from them without the knowledge of the person concerned, **at the request of the President of the Federal Criminal Police Office** or alternatively by **authorisation from the court**[256]. Telecommunications surveillance and online searches[257] may only be **ordered by the court at the request of the public prosecutor's office**. In the event of **imminent danger, the order can also be issued by the public prosecutor's office**. If the order of the public prosecutor's office is not **confirmed by the court within three working days**, it shall become ineffective. The order is to be limited to a **maximum of three months**. An extension by no more than **three months** is permitted insofar as the requirements of the order continue to exist, taking into account the investigation results obtained.[258].

According to sections 100a StPO (telecommunications surveillance) and 100b StPO (online searches), a **range of conditions** need to be met for the court order to be granted, including:

- **Suspicion of an individual based on certain facts**. In the StPO, the fact that an individual has committed a **serious criminal offence** is required[259] . A list of offences considered serious, and relevant regarding intercept orders is given in StPO Section 100a (2) and 100b (2). Sections 100a (3) and 100b (3) stipulate that such an intercept order must be targeted only against the suspect or against persons whom it can be assumed are communicating with the suspect;
- Furthermore, the requests for authorisation **must indicate certain data**. In the StPO, data relevant to the **identity and location** of the person (where known), the **telephone number** or other code

complaint No. 58243/00, Zakharov v. Russia, judgment of the European Court of Human Rights of 4 December 2015, complaint No. 47143/06, Szabo and Vissy v. Hungary, judgment of the European Court of Human Rights of 12 January 2016, complaint no. 37138/14. See section 6.2 for additional detail.

254 Poland, Act on the Police (Ustawa o policji), 6 September 1990, Article 19.16.

255 Poland, Poland, Act on Internal Security Agency and Intelligence Agency (Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu), 24 May 2002.

256 Section 49 (4) BKAG.

257 Sections 100a and 100b StPO.

258 Section 49 (6) BKAG.

259 Sections 100a and 100b).

equipment (e.g. IMEI number / MAC number / IP address), and the **type, extent and duration** of the measure are needed – §100b (2);

- **Intercepted data concerning the core area of the private conduct of life is regarded as off-limits and inadmissible** – Section 100d (4). This section of the StPO states that these data shall not be used, shall be deleted without delay and the fact that they were obtained and deleted shall be documented, with a view to notification (§101 StPO).

Similar to the StPO, the BKAG includes a range of conditions that need to be met for the court order to be granted:

- **Suspicion of an individual based on certain facts**. According to the BKAG, there must be danger to a person's life/freedom or national security (Section 49 (1));
- The requests for authorisation and the order itself **must indicate certain data**. Section 49 (5) and (6) BKAG stipulate the need for the person's name and address; the most accurate description of the measure to be used; the nature, scope and duration of the action to be included in the request; and the main reasons for the use of the measure;
- **Intercepted data concerning the core area of the private conduct of life is regarded as off-limits and inadmissible** - Section 49 (7) BKAG states that, as far as possible, data related to the core area of private life should not be collected. Data that have been collected must be presented to the court issuing the order without delay. The court decides immediately on the usability or deletion of the data. Data that relate to the core area of private life may not be used and must be deleted immediately. The facts of data collection and deletion are to be documented. The documentation may only be used for data protection control purposes. The data is to be deleted six months after the notification pursuant to Section 74 or six months after the court has given its consent to the definitive refraining from the notification. If the data protection control pursuant to Section 69 Paragraph 1 has not yet been completed, the documentation must be retained until it is completed. According to Section 49 (8), in the event of imminent danger, the President of the Federal Criminal Police Office or his or her deputy may decide on the use of the findings in consultation with the Federal Criminal Police Office's data protection officer. When examining the collected data, he or she can use the technical support of two other employees of the Federal Criminal Police Office, one of whom must be qualified to hold judicial office. The employees of the Federal Criminal Police Office are sworn to secrecy about the knowledge they become aware of which may not be used. The court decision according to paragraph 7 must be made up for immediately.

In the case of intelligence agencies, the ex-ante procedures to monitor and record telecommunications differ. The request must be done in writing by the head or deputy of one of the 19 agencies entitled to do so (the BND, the BfV, the MAD and the 16 state-level LvF). In the case of the three federal agencies, the request is sent to the Federal Ministry of the Interior, otherwise, the request is approved by the relevant state supreme authority.[260] Any measure must be approved by a specific Commission, the G10 Commission. The Commission is composed of five members, at least three of whom must be qualified to hold judicial office appointed by the Parliamentary Oversight Panel (*Parlamentarisches Kontrollgremium – PKGr*). The approval of the G10 Commission is necessary for the use of the interception techniques that are to be used.[261] In urgent cases, the relevant ministry may allow for a

[260] G10 act, articles 9 and 10,

[261] G10 act, article 15.

measure to be implemented without prior approval of the G10 Commission. In such cases, the chair of the Commission, her deputy or a member designated by the chair, must confirm the urgency of the order, otherwise the urgent execution of the order is suspended, and the data collected immediately deleted.[262]

The **Federal Intelligence Service** (BND) may **use technical means to process the personal content data of foreigners abroad** on the basis of previously ordered strategic intelligence measures used for the political briefing of the Federal Government or for the early detection of dangers of international importance from abroad (Section 19 BNDG). According to Section 34 BNDG, the BND is authorised to carry out **online searches of foreigners abroad**. Measures must be ordered by the President of the Federal Intelligence Service or by a representative appointed by the President of the Federal Intelligence Service. An Independent Control Council examines the legality of ordering strategic intelligence measures before they are implemented. If the Independent Control Council does not confirm the legality of the order, the order shall become ineffective.

Online searches of the Federal Intelligence Service (BND) require the **prior approval of an Independent Control Council**, which consists of former judges of the Federal Court of Justice and the Federal Administrative Court, who are elected by the Parliamentary Control Committee of the Bundestag on the recommendation of the Federal Government (Section 37 Para. 4, Section 43 BNDG).

5.5.2. Ex-post – sanctions and remedies

In addition to the abovementioned *ex-ante* conditions, there are two key *ex-post* mechanisms of supervision and oversight of hacking practices:

- **Notification of persons targeted:** In criminal cases, as documented in the StPO Section 101, it is a legal requirement to notify persons affected by a telecommunications interception or online search order regardless of the use of the data collected in a criminal court case. It is stated in Section 101 (5) that "notification shall take place **as soon as it can be effected**"[263] without endangering the investigation, persons involved or significant assets. In cases of **deferred notification**, this must also be documented in the investigative file and approved by the court if deferral goes beyond 12 months. It is also necessary to delete and document the deletion of any personal data no longer necessary for the purposes of the criminal prosecution – pursuant to Section 101 (8). According to Section 101 (7), the persons investigated can apply to the competent court for a review of the legality of the measure and the manner in which the investigation was carried out up to two weeks after they have been notified, even after the measure has ended. In the case of communication interception by intelligence agencies, the G10 law sets out that targets of interception must be informed of the measure taken against them once it is finished, except in cases where a threat still exists, as judged by the G10 Commission[264].
- **Reporting:** As detailed in StPO §101b (1), each Länder and the Federal Public Prosecutor General are required to submit an **annual report** to the Federal Ministry of Justice. Regarding Sections 110a and 100b StPO, these reports should include: i) the number of proceedings in which telecommunications interception and online search measures were ordered[265]; ii) the number of surveillance orders, separated by initial order and extension order; iii) the underlying criminal

[262] G10 act, article 15a.
[263] Section 101 (5) StPO.
[264] G10 Act, article 12.
[265] Section 101b (2) and (3) StPO.

offence of the proceedings; and iv) the number of proceedings in which an intervention in an information technology system used by the person concerned as actually carried out. The Federal Ministry of Justice is then required to produce a country-wide summary of these measures. These data are publicly available.[266] The Ministry of the Interior must report at least biannually to the Bundestag's Parliamentary Oversight Panel on the use of G10 powers.

Beyond these provisions, the BKAG (Section74 (6)) stipulates that **persons affected** by covert intervention in information technology systems according to Section 49 BKAG **have to be notified**. According to Section 74 (2) BKAG, notification is given as soon as this is possible without endangering the purpose of the measure, the existence of the state, the life, limb or freedom of a person or things of significant value whose preservation is required in the public interest. If criminal investigations are conducted because of the underlying facts, the criminal prosecution authority decides in accordance with the provisions of criminal procedure law whether notification is to be made. The notification is made by the Federal Criminal Police Office. If the notification is postponed for one of the aforementioned reasons, this must be documented. According to Section 74 (3) BKAG, if the notification deferred in accordance with paragraph 2 is not made within six months of the end of the measure, further deferment requires the court's approval. The court determines the duration of the further deferral, but in the case of Section 49 no longer than six months. Extensions of the deferral period are permitted. Five years after the end of the measure, the notification can finally be waived with court approval if the conditions for the notification will not be met in the future with a probability bordering on certainty, further use of the data against the person concerned is excluded and the data has been deleted.

Finally, according to Section 82 BKAG (**Logging of covert and intrusive actions**), the target person and the people affected and the information for identifying the information technology system and the changes made to it, which are not just fleeting, must be logged.

According to the BNDG, in cases where the BND collects personal data from foreigners abroad, the data subject is generally **not informed** (Section 59 (1) BNDG). In cases where data have been collected from German nationals, domestic legal entities as well as persons residing in federal territory and have not been immediately deleted according to Paragraph 19 (7), the G-10 commission has to be informed in its next meeting, and **the person concerned has to be notified** once the measure has come to an end. However, this can be omitted as long as a threat to the purpose of the restriction cannot be ruled out or as long as the occurrence of overarching disadvantages for the welfare of the federal government or a state is foreseeable[267]. If the notification is not made within twelve months of the collection of the data, further deferral of the notification requires the consent of the G10 Commission[268].

The BVerfSchG (Paragraph 9 (3)) specifies that the Federal Office for the Protection of the Constitution will **inform the person concerned** about the covert use of technical means as soon as a threat to the purpose of the intervention can be ruled out. In addition, the BfV has to inform Parliamentary Control Committee.

The activities of the BKA and the German intelligence services are subject to **judicial control** and the technical and legal supervision of the government departments responsible for them (such as the Federal Chancellery, the Federal Ministry of Interior, the Federal Ministry of Defence). For the

[266] Official note: Statistics available at: https://www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument44152

[267] Paragraph 12 Section 1, G-10 law

[268] Paragraph 59 BNDG

parliamentary control of the Federal intelligence agencies (BND, BfV and MAD), the Bundestag's **Parliamentary Oversight Panel** is the parliamentary oversight mechanism. Among its tasks is the scrutiny of the federal intelligence agencies and the selection of members of the G10 Commission. The Ministry of the Interior shall also inform the committee of the implementation and use of the G10 act at least biannually.[269]

5.6. France

5.6.1. Ex-ante – oversight

The use of special investigative techniques (including hacking of electronic devices) is allowed in French law. There are two main ways in which these techniques can be used by law enforcement authorities. Either this can be done at the request of the police and authorised by the investigative judge (juge d'instruction), or the public prosecutor may request the use of the techniques in which case it must be authorised by the liberty and custody judge (juge des libertés et de la détention). The Code of Criminal Procedure provides for the following *ex-ante* requirements:[270]

- **Article 706-102-1** states that a technical instrument (dispositif technique) for electronic surveillance can be ordered by the investigative judge or the public prosecutor;
- **Article 706-102-3** states the information that should be provided in a request for the use of hacking techniques. Such a request should stipulate the offence that motivates the use of such techniques, the exact location or detailed description of the device to be accessed and the duration for which such techniques will be used.

The use of special investigative techniques is permissible for offences falling within the scope of Articles 706-73 and 706-73-1 of the code of criminal procedure.[271] These articles provide a wide list of crimes, ranging from the facilitation of the illegal entry on the French territory and money laundering to trafficking and terrorism.

Additional provisions in the Code of Criminal Procedure relate to ensuring **access** to protected data on devices already seized. For such cases, **Articles 230-1** and **230-2**[272] stipulate that the public prosecutor or the investigating judge may request the services of a qualified individual or the Centre for Technical Assistance, a classified organisation, to access the data.

Furthermore, once access has been obtained using hacking tools, the Code of Criminal Procedure also governs the **safeguards** related to the collection and use of data (e.g. intercepting communications, copying stored data, handling collected data, etc.). Key provisions in this regard include section 3 of Chapter I of Title III of Book I (Articles 92 to 100-7), which concerns the inspections of premises, searches, seizures and interception of correspondence by telecommunications[273]; Article 100 provides that for cases where the penalty if found guilty exceeds three years' imprisonment, that the investigating judge may order the "interception, recording and transcription" of electronic communication. It states that

[269] G10 act, article 14.

[270] Code de procédure pénale, articles 706-102 and 706-102-3.

[271] Code de procédure pénale, articles 706-73 and 706-73-1.

[272] Code de procédure pénale, articles 230-1, 230-2.

[273] Code de procédure pénale, articles 92 to 100-7. Unofficial translation by John Rason Spencer QC, Professor of Law at the University of Cambridge, available at: http://www.legislationline.org/documents/section/criminal-codes/country/30.

the decision to allow these interceptions has to be done in written form and that no challenge is permissible.[274]

Article 56, which relates to the seizure and recording procedures for the handling of seized computer data; and Article 60-3, which permits the employment of technical experts by the prosecutor to exploit protected data without impairing its integrity. Similar provisions exist in Article 156 for use by investigating judges.

In terms of the use of spying techniques by intelligence and security services, the main **oversight** mechanism is the ***Commission nationale de contrôle des techniques de renseignement (CNCTR)***, whose role is to ensure that intelligence gathering is undertaken legally, following the Code of Internal Security (Code de la Sécurité Intérieure). The CNCTR is composed of four parliamentarians (two MPs and two senators), two members of the Conseil d'Etat (Council of State), two magistrates, one expert in electronic communication techniques.[275] The Commission provides opinions on the use of intelligence gathering techniques. These **opinions are not binding**. In order to undertake their work, the Commission has access to all demands for the use of these techniques and authorisations.

5.6.2. Ex-post – sanctions and remedies

French legislation also includes **several *ex-post* conditions for oversight and supervision** of hacking practices. Articles 56 and 60 of the Code of Criminal Procedure refer to Article 163 and 166, which contain general provisions on the use of **technical experts** to provide access to protected evidence. Article 163 ensures a court inventory of the electronic evidence to be exploited by technical experts. Furthermore, Article 166 states that experts conducting such exploitation operations shall author a report which contains a description of the operations and their conclusions. Both the inventory and the reports shall be provided to the court and recorded via the 'procès-verbal'.[276]

Three main organisations are involved in the ex-post oversight of special investigative techniques. They are:

- The **CNCTR**, presented above, undertakes controls of the intelligence collection techniques from intelligence agencies. The Commission has access to all the intelligence collected in order to control whether this has been done in line with the legal framework. There is **no enforcement mechanism**. The Commission also published an **annual report** setting out the extent to which the law is followed by intelligence agencies;
- The National Commission on Informatics and Liberty (**Commission nationale de l'informatique et des libertés – CNIL**), France's data protection authority. The CNIL's role includes controlling that the law is abided by in terms of the data processing, in particular by IT systems; support citizens in accessing information about personal data processed by organisations and bodies, including those of internal security, intelligence service and the police.[277] The CNIL can provide binding sanctions against state bodies in cases where illegal surveillance has been proven;
- The Defender of Rights (**Défenseur des Droits** – DDD), is France's Ombudsperson. The Défenseur role includes supporting policy makers by providing guidance of proposed laws. The Défenseur is

[274] Code de procédure pénale, article 100.

[275] Article L831-1 Code de la sécurité intérieure.

[276] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.

[277] See CNIL website, available at: https://www.cnil.fr

competent for ensuring security professionals (including law enforcement officials) follow rules set out in law.

France is one of the countries in which there is an **ongoing criminal judicial investigation** in response to four complaints filed. In July 2022, an **investigative judge** was appointed following an inquiry launched by the public prosecutor. The lines of inquiry include criminal association (*association de malfaiteurs*), invasion of privacy, and the fraudulent use of automated data processing systems.[278] The legal challenge will be a test of the functioning of redress mechanisms against hacking and surveillance in France.

Another investigation was initiated after a complaint by two journalists from Mediapart whose phones had been infected by Pegasus. The charges include violation of private life (atteinte à l'intimité de la vie privée, hacking (piratage informatique), correspondence interception (interception de correspondances) and conspiracy (association de malfaiteurs). The public prosecutor delegated the inquiry to a **specialised branch of the French police**.[279] The case is pending.

5.7. Italy

5.7.1. Ex-ante – oversight

The ex-ante oversight mechanisms in Italy on the use of special investigative techniques by law enforcement are stipulated in in the **Code of criminal procedure**. When law enforcement authorities want to use these techniques, they must ask the public prosecutor who in turn has to **ask the judge for the authorisation to use the special investigative techniques** listed in article 266 of the code of criminal procedure. The authorisation may be granted when there are **serious indications of a crime** and **the interception is absolutely essential** for the prosecution of the investigation. In case of **urgency**, the public prosecutor may authorise the use of these techniques without the prior approval or a judge. In such cases, the prosecutor has 24 hours to inform the judge, who must rule on its validity with 48 hours.[280]

The **2017 Orlando reform**[281] addressed a gap in the existing legislative framework to strengthen the safeguards on the use of on interceptions including **spyware** (*captatore informatico*, referred to as *Trojan di Stato* in the Italian debate. The law introduced provisions such as:

- Trojans must be directly operated by **law enforcement** (i.e. not private contractors);
- Every operation that uses a trojan must be duly **logged** and documented in a tamper proof, verifiable way so that the operation's results can be contested by the defendant;
- Once installed, a trojan shall not reduce a device's security level;

[278] See FranceInfo TV, Projet Pegasus : l'enquête française sur le logiciel espion confiée à un juge d'instruction, July 2022, available at : https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/projet-pegasus-l-enquete-francaise-sur-le-logiciel-espion-confiee-a-un-juge-d-instruction_5233438.html

[279] Mediapart, Pegasus : une enquête ouverte à Paris, le début d'un long chemin devant la justice, July 2021, available at : https://www.mediapart.fr/journal/international/200721/pegasus-une-enquete-ouverte-paris-le-debut-d-un-long-chemin-devant-la-justice

[280] Article 267 Codice di Procedura Penale 2022, available at: https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-di-procedura-penale own translation

[281] Decreto legislativo 29 dicembre 2017, n. 216, available at: https://www.gazzettaufficiale.it/eli/id/2018/01/11/18G00002/sg

- The use of the tool is "strictly limited" to investigations into **organised crime**, and targeted to individuals or a **specific setting** (e.g. room, building);
- **Data** accessed using such a tool "must be stored in the prosecutor's servers and must be protected from third-party access" with encryption; and
- Non-relevant data must be screened and deleted.

Decree Law 161 of 2019 restructures the management of intercepted data and, above all, expands the categories of crime for which computer detectors can be used and introduces the obligation for companies that supply these surveillance systems to use encrypted systems and securely delete files.[282]

In a 2020 landmark case, the Corte di Cassazione[283] ruled, *inter alia*, that ex-ante safeguards do not require the request to use a spyware to indicate a specific place, as this is neither indicated in the Italian Code of Criminal Procedure, nor introduced by ECtHR jurisprudence.[284] This jurisprudence increase the possibility of using spyware to and the admissibility of the evidence collected in court, regardless of where the phones hacked is located, including in the home.

5.7.2. Ex-post – sanctions and remedies

In addition to the above *ex-ante* provisions, the law introduces a range of *ex-post* supervisory provisions.

For intelligence services, the ex-post mechanisms are set out in Law No. 124 of 3 August 2007.[285] The law has created **Parliamentary Committee for the Security of the Republic (*Comitato parlamentare per la sicurezza della Repubblica* - COPASIR)**, entrusted with more detailed and pervasive powers of oversight on the activities of the two intelligence agencies. COPASIR is composed of five members of the chamber of deputies and five senators.

The Committee has the powers to

- Declassify State Secrets;
- Acquire acts and dossiers from judicial investigations, with the authority to overcome the professional secrecy;
- Have free access to intelligence agencies' offices and documentations.

The Orlando law included ex-post mechanisms, including a requirement to notify individuals that have been the subject of invasion by hacking tools, that they have the right to examine the information collected.[286] The judge is in charge of removing data which is either not relevant or includes personal data from the records.

---

[282] Freedom House, Freedom of the Net report 2022, Italy, available at: https://freedomhouse.org/country/italy/freedom-net/2022

[283] Italian Court of Cassation, Decision Num. 31604, 30 September 2020 available at: https://penaledp.it/app/uploads/2021/02/Cass.-Sez.-V-30-settembre-2020-dep.-11-novembre-2020-n.-31604-.pdf

[284] See an analysis of the case Murone, Emanuele Salvatore, Brevi note sul rapporto tra trojan horse e libertà di autodeterminazione, available at: https://www.penaledp.it/brevi-note-sul-rapporto-tra-trojan-horse-e-liberta-di-autodeterminazione/

[285] LEGGE 3 agosto 2007, n. 124, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2007;124

[286] Decreto legislativo 29 dicembre 2017, n. 216, available at: https://www.gazzettaufficiale.it/eli/id/2018/01/11/18G00002/sg

The Orlando law introduced the creation of a National Trojan Registry, which held a 'fingerprint' of each version of the software and the Trojan's source code having to be deposited to a specific authority. This has been replaced in 2019 with a digital archive under the supervision of the Public Prosecutor. The archive can be accessed by the prosecuting judge, the public prosecutor, and the defendant. Access to the digital archive is logged.[287]

5.8. Netherlands

5.8.1. Ex-ante – oversight

The use of lawful intercept or hacking in the framework of the criminal procedure is regulated by the Computer Crime Act III, which does include the requirement for the **public prosecutor to submit a written request** asking for a **written prior authorisation (*machtiging*) to the investigative judge**, before giving an order for hacking.[288] The authorisation needs to state the details of the hacking order and the period for which hacking is authorised. However, while the start of a hacking operation requires prior written authorisation, Article 126nba (5) allows that extensions of the authorisation of the investigative judge can be provided **orally** in "urgent need", as long as the authorisation for the extension is eventually provided in written form within three days.

The decision is taken on the basis of a proportionality assessment and both the request by the public prosecutor and the authorisation decision of the investigative judge must be motivated on this basis. The Explanatory Memorandum of the law further requires the **Central Review Commission** (*Centrale Toetsings Commissie*) to provide advice to the investigative judge before it takes its decision. Moreover, the technical means proposed are assessed against several legal safeguards under the 2006 Decree of technical tools.[289]

Article 126nba (3) of the Code of criminal procedure states that the order for the special investigative power of hacking can only be provided for a **maximum period of four weeks** and can be extended for a maximum period of four weeks at a time.

Article 126nba (2) requires the prosecutor's order for law enforcement to hack as part of an investigation to include the following details:

- The alleged crime and (if known) the name of the suspect;
- The number or another identifying description of the computerised device to be hacked;
- The circumstances which show that the crime is a 'serious breach of law', and that the investigation needs the hacking 'urgently';
- A description of the type and functionality of the technical means to be used;
- The purpose of the hacking and, in some cases,[290] a description of the acts to be undertaken;
- Which part of the computerised device and which categories of data are included;
- The time or time period for which the order is given;

[287] Altalex, Intercettazioni, il decreto-legge di modifica della disciplina, September 2020, available at: https://www.altalex.com/documents/leggi/2020/01/02/intercettazioni

[288] Artikel 126nba (4), Gewijzigd Voorstel van Wet – Computercriminaliteit III, 20 December 2016.

[289] Besluit technische hulpmiddelen strafvordering, available at: http://wetten.overheid.nl/BWBR0020444/2013-03-15.

[290] If for the purpose of article 126nba (1) 9a), (d) or (e) Wetboek van Strafvordering.

- Whether or not a technical means is to be applied on a person.

Under Article 126nba of the Code of Criminal procedure,[291] hacking can only be requested by the public prosecutor for investigations:

- into crimes described in **Article 67(1)** of the Dutch Code of Criminal Procedure (crimes for which the maximum sentence is four years or higher, or some specifically designated crimes with a lower maximum); and
- into crimes that are **serious breaches of law;** and
- when **the investigation requires this urgently**; and
- for the purpose of:
    - establishing certain characteristics of the automated device of the user (e.g., the identify or location);
    - to execute an order as described in Article 126l (recording private communications by using a technical aid) or 126m of the Criminal Procedure Code (recording private communications which take place using services provided through a communications provider, by using a technical aid);
    - to execute an order as described in Article 126g of the Criminal Procedure Code (systematic observation, incl. by attaching a technical aid to a person);
    - recording of data that are stored in the automated device;
    - making data inaccessible (as described in Article 126 cc (5) of the Criminal Procedure Code).

In practice this article allows law enforcement to **enter** a computerised device that is used by a suspect and **search** the device with the purpose of:

- Undertaking an online search (stored data), including looking at the data and copying the data, as well as making data inaccessible;
- Intercepting private information (streaming data), including capturing keystrokes (incl. passwords) and real-time monitoring of data traffic (which may or may not include encryption);
- Influencing the data, by adjusting settings, turning on webcams / microphones, sabotaging or turning a device off.

Moreover, the law allows law enforcement to provide itself with access to / enter the computerised device in different ways, including:

- Using a vulnerability in the IT system;
- Enter / intrude using a false identity or by brute force;
- Use a trojan to infect the device with malware.[292]

If the hacking is undertaken for the purpose of copying or deleting stored or incoming data, the offence to which the hacking relates needs to be an offence which carries a sentence of eight years or more.

[291] Artikel 126nba, Gewijzigd Voorstel van Wet – Computercriminaliteit III, 20 December 2016.

[292] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.

The information collected through hacking **may be used as evidence during the criminal investigation and during the trial**. The Memorandum of Understanding of the hacking law states that in order to check which hacking activities were undertaken, law enforcement needs to log their hacking activities in the automated device.[293] It further states that the requirements around this 'logging' will be included in the Decision on technical aid (Besluit technische hulpmiddelen strafvordering) (the Memorandum also notes that any activities undertaken by the police officer need to be included in the 'proces-verbaal' (a statement of the facts of the case), referring to Article 152 of the Dutch Code of Criminal Procedure. However, the statement does not include information on the software that was used to undertake the hacking.

The use of lawful intercept or hacking by Dutch **intelligence and security services** requires a **three-step authorisation**. This first one is for investigators to convince their internal **jurists** of the validity of the need for the use of the special investigative technique. Once this is done, they must seek the approval of the **Minister** in charge of the services (Ministry of Defence or of the Interior). The final step is the **Investigatory Powers Commission** (*Toetsingscommissie inzet bevoegdheden* - TIB), whose role is to assess the legality of the approval. The TIB's decision is binding. The TIB is composed of two judges and one technical expert.[294] The TIB's ex-ante role and the binding nature of its decision has made is a model which other countries have been trying to emulate.[295]

5.8.2. Ex-post – sanctions and remedies

The national law does not require *ex-post* supervision or oversight by judicial or other bodies but assumes that *ex-post* oversight will take place when the case goes to trial and the evidence resulting from the investigation measures is tested in court. The Computer Crime Act III includes a provision (art. 126nba (7)) foreseeing ***ex-post* monitoring by the Inspection of Public Order and Safety (*Inspectie Openbare Orde en Veiligheid)***.[296] However, according to Bits of Freedom this oversight is not independent judicial oversight as described in European jurisprudence. Moreover, the law is unclear on what the oversight by this Inspection would exactly entail.[297]

As stated above, the 'proces-verbaal', which is a statement of the facts of the case, includes information on the special investigative powers, such as hacking, used in the particular case. The suspect and his/her lawyer can take note of this document in preparation for the trial. In the event that they perceive these investigative powers to be used unlawfully, they could argue this in court.

Dutch law places an **obligation on law enforcement agencies to notify the suspect** of their use of hacking **once the investigation is over** and insufficient evidence has been found to continue the investigation or to bring the case to court.[298] Another way for the use of the hacking power by the police to become public is if the case goes to court and one of the grounds of the lawyer was the unlawful use of the investigative power of hacking (procedural defect) and the judgement is made public.

---

[293] Memorie van Toelichting Wet Computercriminaliteit III, 2015, Section 2.6.

[294] See Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017), articles 32-37, available at: https://wetten.overheid.nl/BWBR0039896/2022-05-01

[295] See tagesschau, Kontrollrat soll Abhöraktionen überwachen, available at: https://www.tagesschau.de/inland/bnd-353.html

[296] See also article 65 Politiewet.

[297] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.

[298] Article 126bb Wetboek van Strafvordering.

In relation to surveillance by intelligence agencies, the **Review Committee on the Intelligence and Security Services** (CTIVD) is tasked to verify the lawfulness of the actions of the AIVD and the MIVD, as well as of the actions performed on behalf of these services by other government bodies (such as the police) as was the case for the Taghi case (see section 3.8)). It produces an annual report which is presented to the Parliament and the Committee for the Intelligence and Security Services. The CTIVD is the ex-post oversight mechanism set out in the Intelligence and Security Services Act 20172017. It includes an Oversight Department, which has direct and independent access to all data processed in the context of the activities carried out in application of this law. In the course of its investigations, the Oversight Department has direct access to all digital and physical information systems of both the AIVD and the MIVD. The Oversight Department establishes of its own accord which information and which cooperation it deems necessary.[299] The Review Committee on the Intelligence and Security Services (CTIVD) is composed of four members appointed by royal decree on the recommendation of the House of Representatives.

[299] CTIVD Oversight Department, investigation protocol oversight, available at: https://english.ctivd.nl/binaries/ctivd-eng/documenten/publications/2019/06/19/oversight-protocol/CTIVD+Oversight+protocol.pdf

6. FUNDAMENTAL RIGHTS CONSIDERATIONS

6.1. Fundamental rights set out by the Charter and the ECHR as interpreted by the courts

As stipulated in the **Charter of Fundamental Rights of the European Union** (Article 7) and the **European Convention on Human Rights** (Article 8), the **right to privacy** is a qualified right, meaning that it can be lawfully restricted under certain, specified circumstances. Other rights enshrined in the **Charter of Fundamental Rights of the European Union** may be affected by the use of spyware by state actors. These rights include the right to see one's personal data protected (article 8), the right to the freedom of expression (article 11). In addition, other rights may be affected, including non-discrimination (article 21) and the right to a fair trial (article 47).A **restriction** of these rights must be:[300]

- In accordance with **law**;
- **Necessary and proportionate**; and
- For one or more of the following **legitimate aims**:
  - the interests of **national security**;
  - the interests of **public safety or the economic well-being** of the country;
  - the **prevention of disorder or crime**;
  - the protection of **health or morals**; or
  - the protection of the **rights and freedoms of others**.

This is not a new concept. Coercive law enforcement activities have restricted the right to privacy based on appropriate legal provisions for hundreds of years (e.g., the Fourth Amendment of the US Constitution, as passed in 1789[301]). However, it is widely recognised that the use of spyware such as Pegasus has the potential for **increased invasiveness** when compared with traditional coercive activities (e.g., wiretapping, house searches etc.). The use of such tools can provide law enforcement or intelligence agencies with access to all data held on a device, all information flows in and out of the device as well as having the potential to record video and audio in any location. This is likely to constitute the collection of a much greater amount of data, as well as the collection of much more sensitive data. Article 52(1) of the Charter of Fundamental Rights recognises the need to restrict the fundamental rights of individuals to the extent that they are proportionate and necessary.

As long as the hacking practices are necessary to overcome the 'Going Dark' problem and proportionate to fulfilling this aim, national-level legal frameworks may restrict the right to privacy through the legal stipulation of appropriate limitations and safeguards considering the above points.

A key consideration is that by their secretive nature, the use of interception measures in general cannot be questioned by those affected, as they are unaware of the fact. Furthermore, this study has found a number of shortcomings in the national legal framework for the use of spyware by state actors. It is therefore important to refer to standards set out by the CJEU interpreting the EU Treaties and the Charter on Fundamental Rights, the ECtHR, interpreting the ECHR as well as other international bodies such as the Venice Convention.

[300] Liberty Human Rights. Article 8 Right to a private and family life. Available at: https://www.liberty-human-rights.org.uk/human-rights/what-are-human-rights/human-rights-act/article-8-right-private-and-family-life.

[301] Friedman, B. and Kerr, O. Common Interpretation: The Fourth Amendment IV. Available at: https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv.

Relevant CJEU cases include the following:

- The *Digital Rights Ireland and Others case (*C-293/12 and C-594/12, Judgment of 8 April 2014)[302]. In this case, the Court was asked to examine the compatibility of the Data Retention Directive (Directive 2006/24/EC) with article 7 and 8 of the Charter of Fundamental rights (on the Right to Privacy and the Right to Data Protection). The court clarified the principle of necessity and proportionality in using the interference restrict the fundamental rights of individuals (as per article 52(1) of the Charter of Fundamental Rights).
- The *Schrems II case* (C-311/18, *Facebook Ireland and Schrems („Schrems II"), Judgment of 16 July 2020*)[303]. In this case, an Austrian national and Facebook user filed a complaint requesting his personal data not to be transferred to the USA in light of the social media's lack of protection against mass surveillance activities in which public authorities were engaged. The Court found that "*the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned*" (para 175).
- The *Quadrature du Net case*. (C-511/18, C-512/18 and C-520/18, Judgment of 6 October 2020). In these joint cases, advocacy groups asked the Court to assess the lawfulness of legislation adopted by Member States in the field of the processing of personal data in the electronic communications sector, for the purposes of protecting national security and combating crime. The court ruled that genuine threat to national security could justify very serious interferences with fundamental rights as long as the conditions in which this is done are strict and the safeguards exist.
- The *Privacy International case* (C-623/17 - Privacy International, Judgement of 6 October 2020)[304]. The question the Court was asked to rule on was whether EU law applies to bulk communications data collection by intelligence agencies for national security purposes. The CJEU agreed that national security objectives can justify more serious interference with fundamental rights than other objectives such as fighting organised crime (para 75, as per the *Quadrature du Net* case). However, the court did reiterate that "*the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable*" (para 44). In other words, EU law sets out privacy safeguards regarding the collection of data by national governments, which countries must follow.

The ECtHR has also developed a doctrine interpreting the ECHR through its jurisprudence on the use of surveillance techniques. It has found that "the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications was, under exceptional conditions, necessary in a democratic society" (*Klass and Others v. Germany*)[305]. The Court does, however, require the law to have sufficient **clarity** to provide adequate protection against abuse of power (*Liberty and*

[302] Judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, available at: https://curia.europa.eu/juris/liste.jsf?num=293/12&language=en .

[303] Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, available at: https://curia.europa.eu/juris/liste.jsf?num=C-311/18 .

[304] Judgement of 6 October 2020, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (C-623/17), available at: https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-623/17 .

[305] *Klass and Others v. Germany*, Application no. 5029/71, judgement of 6 September 1978, available at: https://hudoc.echr.coe.int/eng?i=001-57510

Others v. the UK)[306]. In a series of landmark cases, the Court found that legal provisions governing interception of communications must provide for "**adequate and effective guarantees** against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance" (*Roman Zakharov v. Russia*).[307] It also recognised that "governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents", but that this must be done with **sufficient safeguards, including ex-ante mechanisms or remedies** (*Szabó and Vissy v. Hungary*)[308].

In *Ekimdzhiev and Others v. Bulgaria*[309], the Court found that the existing laws regarding the secret surveillance and the retention and accessing communications did not meet the **quality-of-law** requirement of the Convention. In both the *Szabó and Vissy*, and *Ekimdzhiev and Others* cases, the Court asked the respective governments to make the necessary changes to domestic law to end the violation.

Overall, the jurisprudence of the CJEU and ECtHR can be summarised to state that **limitations of Fundamental Rights may be justified under certain conditions.** The limitations must be clearly set out in law and respect the spirit of the rights affected. They must be proportionate and only imposed if strictly necessary. Above all, they must meet general interest objectives either set out by the EU or necessary to protect the rights and freedoms of others. The prevention of serious crimes, as well as a genuine threat to national security objectives can be justify interferences with Fundamental Rights. In this case, safeguards must be in place, in particular on the proportionality of the interference with the threat.

6.2. Other international standards

The Venice Commission is the Council of Europe's advisory body on constitutional matters. Part of the work of the Commission revolves around the oversight of certain bodies in functioning democracies. In particular, the Commission has developed reports on the Democratic Oversight of the Security Services[310] and of Signals Intelligence Agencies[311] These two documents set out standards that must be followed in order for security and intelligence services to operate effectively while respecting democratic principles.

With regards security services, the Venice Commission focuses on accountability, which is understood in this context as "*being liable to be required to give an account or explanation of actions and, where appropriate, to suffer the consequences, take the blame or undertake to put matter right, if it should appear that errors have been made*".[312] It identifies two main areas of accountability, namely parliamentary and judicial accountability. Given the high degree of secrecy accompanying the work of secret services, accountability is a difficult to achieve. It requires a level of subjectivity in the assessment by

[306] *Liberty and Others v. the UK*, Application no. 58243/00, judgement of 1 July 2008, available at: https://hudoc.echr.coe.int/fre?i=001-87207

[307] *Roman Zakharov v. Russia*, Application no. 47143/06, judgement of 4 December 2015, available at: https://hudoc.echr.coe.int/eng?i=001-159324

[308] *Szabó and Vissy v. Hungary*, Application no 37138/14, judgment of 12 January 2016, available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}

[309] *Ekimdzhiev and Others v. Bulgaria*, Application no. 70078/12, judgement of 11 January 2022, available at: https://hudoc.echr.coe.int/fre?i=001-214673

[310] European Commission For Democracy Through Law (Venice Commission), Report On The Democratic Oversight Of The Security Services, adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007), updated by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015).

[311] European Commission For Democracy Through Law (Venice Commission), Report On The Democratic Oversight Of Signals Intelligence Agencies, adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015).

[312] Op. Cit. Venice Commission, Security Services, p.16.

organisations exercising oversight. The Commission identifies, ways in which these difficulties can be overcome. First, it suggests that rules on the mandate of the security organisations are clear and concise and that they are only kept secret if absolutely necessary.

Internal control of the agency is identified as the main guarantee against abuses of power. This can be influences by the quality of the staff and its commitment to democratic principles, the existence of an independent official designed to oversee the agency, clear internal rules on decision-making processes.

In term of **parliamentary accountability**, the Venice Commission's standards include:

- The fact that members of the oversight body need to possess **adequate expertise;**
- An oversight body which reports to parliament should be able to **decide when and how often to report and what is included in the report**;
- **Autonomy should be the guiding principle of any oversight body**. This include having members from different parties as well as a clear demarcation between the oversight body and the agencies overseen.[313]

In terms of **judicial accountability**, the judges must be **independent**. Furthermore, they should possess the necessary expertise. **Specialist training** is advisable as otherwise they may not be able in practice to question the experts' threat assessments. The Commission does however point that "**case-hardening**" (a tendency of the specialised judges to identify with the security officials) must be avoided and recommends that judges remain in place for a limited period of time.[314]

Given the challenges linked with the accountability of security services, the Venice Commission also lists 'supplement' or replacement mechanisms in the form of 'expert accountability' and 'compliant mechanisms'. **Expert bodies** can allow for greater expertise and time to be devoted to oversight, and do not present the same risks of political division as a parliamentary body. Their mandate can also be tailored to the agency there in charge of overseeing. The Commission suggests that member of expert bodies should be trained in the relevant field (law, technology etc.). One important dimension of expert bodies is that they need to be trusted by parliament and the public at large.[315]

Finally, the Venice Commission talks of the 'clear necessity' for the possibility for a victim to seek redress before an independent body. It also highlights how ordinary courts' ability to serve as an adequate remedy in the field of security is limited.[316]

With regards Signals Intelligence Agencies, the Commission sets out recommendations that are more specific than those of security services. While there are many overlaps, the specificities of signals intelligence (involving access to Internet and telecommunications content and to metadata) calls for more specific recommendations as listed below:

- There is a higher **likelihood of conflict of jurisdiction** between the state collecting the information, where the target is located or their nationality. As such the Commission calls for minimum international standards;[317]

[313] Ibid, pp 33-43.
[314] Ibid, pp 44-49.
[315] Ibid, pp 50-54.
[316] Ibid, pp 55-56.
[317] Op. Cit., Venice Commission, Signals Intelligence Agencies, p.28.

- The **mandate** of a signals intelligence agency should be **specific** otherwise there is a risk of ineffective oversight;[318]
- **ECtHR case law should be considered as minimum standards** and countries should endeavour to provide more extensive guarantees;[319]
- **Expert bodies have a particular role to play** in ensuring that signals intelligence agencies comply with high standards of data protection.[320]

6.3. Spyware in particular

Given the new level of intrusiveness of Pegasus and equivalent spyware technologies, there is currently no case law on their use. The capabilities of a smartphone and the ability it has to record images, sounds, and provide its users' locations, makes it a potentially very sensitive device. Gaining access to the contents and features of such a device (as is the case with Pegasus), is, according to the European Data Protection supervisor (EDPS) '**unlikely to meet the requirements for proportionality**' set out by the CJEU.[321] The EDPS further states that the level of interference with the right to privacy in the use of Pegasus and equivalent spyware is so severe that the individual is in fact **deprived of it**. The ability to switch off some features of the spyware to limit the intrusiveness of the spyware leads the EDPS to refrain from completely excluding its use in specific situations. Despite this caveat, **the EDPS is of the opinion the regular deployment of Pegasus or similar spyware would not be compatible with the EU legal order**.[322]

The opinion from the EDPS on the importance of ex-ante and ex-post oversight in the use of spyware and ensuring that the level of intrusiveness is proportional is a key concern. According to Roman Ramirez, a cyber security professor, controlling the use of spyware programmes is the most important issue, which requires the existence of consequence for abuse when fundamental rights are not respected.[323]

Beyond the fundamental rights aspect relating to surveillance, there are concerns about involving **private companies** in intrusive investigation procedures. While fundamental rights primarily bind the state, they do not necessarily affect spyware providers[324]. If private parties can access collected data, it will exacerbate interference with the fundamental right to confidentiality and integrity of IT systems. The Society for Civil Rights (*Gesellschaft für Freiheitsrechte*) lodged a complaint with the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) against the use of the "Pegasus" spy software by the Federal Criminal Police Office (BKA), raising these issues, as well as that of unlawful outsourcing of sovereign powers, insufficient safeguards against unauthorised access and deletion, unlawful commissioning of data processing, insufficient functional limitations, unlawful modifications of the target system, and the illegal exploitation of security vulnerabilities.[325]

---

[318] Ibid, p 16.

[319] Ibid, pp 25-27.

[320] Ibid, pp 33-34.

[321] EDPS, Preliminary Remarks on Modern Spyware, February 2022, available at: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en

[322] Ibid.

[323] PEGA committee hearing Spyware - Use, safeguards and supervision, Monday 13 June 2022.

[324] Klaas A., BKA setzt ums-trit-tene Spy-ware ein, Legal Tribune Online, 14 September 2021.

[325] Moini B., Beschwerde gegen den Einsatz der Pegasus-Software durch das Bundeskriminalamt, Society for Civil Rights, 22 September 2021.

7. CONCLUSIONS AND RECOMMENDATIONS

7.1. Conclusions

The coexistence in democratic societies of the respect of the fundamental right to privacy and the protection of the safety of its citizens creates conflicts and debates that have existed for centuries. The emergence of new technologies has only served to exacerbate the debate. This report provides a focused update on a study on hacking by law enforcement authorities. In 2017, the report concluded on the risks to fundamental rights, the security of the internet and territorial sovereignty of the use of hacking techniques by law enforcement authorities. It further pointed to "substantial criticism" that could be levied against the countries the report focused on based on the lack of clear and effective legal frameworks and oversight mechanisms.[326]

The emergence of spyware such as Pegasus, Candiru, Predator, and equivalent ones raises even more difficult questions. The EDPS suggests that these programmes are 'unlikely to meet the requirements for proportionality' by EU and international standards in the respect for privacy.

Despite this, NSO sold the Pegasus spyware to 14 EU governments, at least three of which have used it against their own citizens in ways that appear to have gone beyond the safeguard requirements by international standards. Other equivalent spyware has been used by other EU government included in this study in similar fashion.

All the countries assessed for this study do have a legal framework restricting the use of spyware to law enforcement and intelligence agencies. The laws on the export of such technologies are generally vague.

It has not been possible as part of this study to confidently confirm the way in which law enforcement or intelligence agencies have access to the use of spyware. Some countries refute the purchase of the spyware licences, while it has despite this been established with a degree of certainty that the countries had in fact used spyware. The opacity of the procurement mechanisms, while arguably necessary for security and intelligence reasons, poses an oversight problem. There is no possibility to assess the capacity of tools and technologies acquired at the procurement stage.

In many cases, the ex-ante mechanisms allowing for the use of Pegasus or equivalent spyware are inadequate. This ranges from cases where the lack of oversight has been established by the ECtHR and not remedied (Hungary), to cases where there is a lack of independent oversight mechanism (Spain, Greece, Poland). Amidst this negative outlook, some good practices have been identified, such as the need for a binding decision by the Dutch TIB before the use of special investigative techniques. This more stringent mechanism also ensures that the organisations entitled to use these techniques identify alternative and more proportionate methods before resorting to using them.

Effective ex-post oversight mechanisms would have uncovered the use of Pegasus and equivalent spyware by law enforcement and intelligence agencies against domestic journalists, politicians and civil rights activists. However, these abuses have instead been uncovered by civil society organisations and investigative journalists. This points to one of the spectacular gaps identified in this report.

In cases where the Ombudsperson looked into the legality of the use of spyware, they have found it to be legal. This points to the need to strengthen or clarify the legal framework, in particular the oversight mechanisms for the use of such investigation techniques.

[326] European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, pp 66-67.

Finally, a number of court cases have been initiated by targets of Pegasus or equivalent spyware or organisations representing them. In all the cases identified in this study, these are targeted at the providers, their owners, and their shareholders, but not at the states using them. This points to an identified need to seek redress and uncover, through judicial means, additional information on the capability and use of the programmes.

7.2. Recommendations

On the basis of the findings of this study we make the following recommendations:

Recommendation 1: Member States who allow the use of special investigative techniques (hacking, use of spyware, etc.) by their law enforcement and/or intelligence agencies, should adopt and implement **clear and effective laws regulating** them in detail, providing for procedural guarantees, ex ante and ex post controls and oversight, through internal procedures, parliamentary scrutiny and judicial review and redress mechanisms. Clear definitions should also be part of those laws (for concepts such as 'national security').

Recommendation 2: Member States should draft or review their laws in a way to respect the requirements developed by the **ECtHR, the CJEU, the Venice Commission and the Council of Europe**, so to ensure that these laws respect Article 2 TEU values and notably democracy, the rule of law and fundamental rights.

In many instances, there is a lack of robustness and independence in the ex-ante mechanisms in place to authorise the use of special investigative techniques. This can be the result of the dichotomy between the speed at which technology advances and the time it takes to develop and adopt legislation.

Recommendation 3: Following up from the experiences of Pegasus and similar spyware scandal, Member States should **refrain from using technologies that have a disproportionate detrimental impact on human rights**. The **proportionality** of the tools used should be a key factor in the decision to acquire and use them. Furthermore, their use and effectiveness should be monitored by an independent body on an ongoing basis.

Recommendation 4: Member States and the European Parliament could encourage the development of a model law on the use of spyware and other intrusive technologies to support countries in the development of a robust legal framework.

Beyond the need to ensure robust oversight mechanisms, the acquisition of technologies which have a detrimental effect should be better regulated. The next set of recommendation relates to the regulation of the market for such technologies.

Recommendation 5: The European Parliament could request the Commission to submit a legislative proposal to require that all surveillance companies domiciled in Member States act responsibly, are held liable for the negative human rights impacts of their products and services, and adapt procurement standards to restrict them to companies which demonstrate that they respect human rights.

Recommendation 6: Companies providing surveillance technologies or services should be asked to make public their aggregated information on surveillance practices including the number of data requests they have received and provided. This would allow civil society organisations and journalists to better understand government practices and provide an important tool for holding governments to account.

Finally, the importance of investigative journalists and civil society actors in the uncovering of the widespread use of Pegasus and equivalent spyware should not be forgotten.

Recommendation 7: The European Parliament should continue its efforts to support the freedom and independence of the press, as well as its efforts to protect whistle-blowers, as their work is the most effective safeguard identified in this study.

8. ANNEX – COMPARATIVE TABLES

	FR	DE	IT	NL	PL	HU	ES	EL
Right to privacy - confidentiality of communica-tions - data protection	- not in the Constitution - Article 9 of the *Code Civil,* - Post and Electronic Communications Code (*Code des postes et des communications électroniques*) - domestic law application of the European Convention on Human Rights. - French Constitutional Court jurisprudence	The right to privacy of correspondence, posts and telecommunications is included in the German Constitution (Basic Law – Grundgesetz §10) and has been highly protected	While the Italian Constitution does not expressly refer to a right to privacy or data protection, the Constitutional Court and Supreme Court regularly defined the privacy as a fundamental human right	The right to privacy is protected by articles 10 (general right to privacy), 11 (inviolability of one's body), and 13 (secrecy of correspondence) of the constitution.	The right to privacy is protected by article 47 of the constitution, with the right the privacy of communications covered by art. 49.	**- in the Fundamental law**	**Constitution recognises the right of privacy of communications**	The Greek constitution enshrines the rights to be "protected from the collection, processing and use, especially by electronic means, of their personal data" (art. 9A)
Definitions Hacking, spyware etc.	**- spying:** capture, saving or transmission of voice, images and geo-localisation information without the knowledge or consent of the person targeted (art. 226-1). - **opening, deleting, slowing or diverting** the transmission […] and **obtaining the contents** of the communication (art. 226-15). **- hacking:** "*to access or stay in a fraudulent manner in all or part of*	**- hacking** (i.e. unauthorised access) according to Sec. 202a and Sec. 202b (so called "**data espionage**", Sec. 202a , and "**phishing**" Sec. 202b). Sec. 202a defines "data espionage" as unlawfully obtaining data for oneself, or another, that was not intended for one and was especially protected against unauthorised access, and circumventing protection.	- **hacking**: art. 615-quarter of the Codice Penale, covers anyone who "*illegally procures, holds, produces, reproduces, disseminates, imports, communicates, delivers, makes available to others or installs equipment in any other way, tools, parts of equipment or tools, codes, keywords or other means suitable for accessing a computer or telematic system, protected by security measures*".	**hacking** is defined as 'computer intrusion" and is defined as the 'unlawful intrusion of automated systems". The crime covers the use of spyware (access by a technical intervention).	- **hacking**: "*whoever without authorisation obtains access to an information not meant for them, by opening a sealed letter, connecting into a telecommunications network, or by breaking or avoiding electronic, magnetic, informatic or other special protection of such network...*" - other related similar crimes (see below sanctions) - phishing	**- hacking: illegal data acquisition** - criminal **offences against information systems**	**hacking** - seizing electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or image, or any other communication signal	**hacking** as the unauthorised access to electronic data, (art. 370B(1), the unauthorized access to information systems or to information transmitted through **telecommunications systems, which (art. 370D(2).**

	FR	DE	IT	NL	PL	HU	ES	EL
	an automated data processing system" - **use of spyware** (article 323-3 of the criminal code): "*fraudulent introduction, extraction, detention, reproduction transmission, deletion or modification of data in an automated data processing system*". - **spyware** (guideline published in the official journal): "*software designed to collect and transmit to third parties and without the knowledge of user data about the user or information relevant to the system she uses*"	- Depending on the case, "hacking" could possibly come under the definition of both of the offences set out above, depending on the level of protection applied to the data in question. .- **Infection of IT systems with malware**			- **infecting IT systems with malware**			
Sanctions (in general, hacking is criminalized in the Criminal Code)	up to three years' imprisonment and a fine of up to EUR 100 000.	- **hacking**: imprisonment not exceeding three years, or a fine. - phishing: imprisonment for up to two years or a fine, unless the offence is subject to a more severe penalty under other provisions	- **hacking** (i.e. the unauthorised access to IT and telematic systems - art. 615-ter): of **up to three years imprisonment**. - **five years in specific cases**	**Hacking** is a crime under article 138ab of the Code of Criminal Procedure is liable to up to two years in prison and a fine of fourth category. When the instruction leads to taking control of a device or the taping of data stored or transmitted from the device, the sanction rises to four years in prison.	- Art 267: imprisonment of up to **two years** for **hacking, eavesdropping**, using visual or other tools or programs, revealing information obtained by means described above to another person. Offences are prosecuted upon the request of the victim. - **fine** of up to EUR 2.3 million	- unauthorised **interceptions**: up to three years' imprisonment - **spyware**: up to two years' imprisonment	**prison sentence of up to four years**	Up to five years' imprisonment

	FR	DE	IT	NL	PL	HU	ES	EL
					- GDPR penalties: up to EUR 20 million or, in the case of an enterprise, up to 4% of its total annual global turnover - **phishing** up to 5 years imprisonment - **infecting IT systems with malware**: up to 5 years imprisonment			
Spyware	**Criminal Code forbids** manufacture, import, possession, display, offer, rental or sale, or installation (art. 226-3).	The infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses) constitutes a criminal offence according to the German Criminal Code ("computer sabotage")	Criminal Code prohibits it (art. 615-quarter) and acts like: *illegally procures, holds, produces, reproduces, disseminates, imports, communicates, delivers, makes available to others or installs equipment in any other way, tools, parts of equipment or tools, codes, keywords or other means suitable for accessing a computer or telematic system, protected by security measures*"	**hacking** is defined as 'computer intrusion" and is **Hacking** is defined as the 'unlawful intrusion of automated systems". The crime covers the use of **spyware** (access by a technical intervention).	- criminal offences under Section 269b of the Criminal Code: **distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime**.	- spyware: up to two years' imprisonment	According to article 197, whoever seizes "electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or image, or any other communication signal", is liable to a prison sentence of up to four years	Infecting an IT system with malware (including spyware) is a criminal offence and covered by different articles of the criminal code depending on the type of infection. This includes art. 292 on crimes against the security of telephone communications, art. 292B on hindering the operation of information systems, art. 370 on the violation of the secrecy of letters
Sanctions on spyware	up to **five** years' imprisonment and a fine of up to EUR 300 000.	up to **five** years' imprisonment	punished by up to **one year imprisonment** and a **fine** of EUR 5 164	up to two years in prison and a fine of fourth category	- Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit cybercrime (e.g. damaging, databases, preventing automatic collection and transmission of data, or hindering access to	- spyware: up to two years' imprisonment	up to four years' imprisonment	up to five years' imprisonment

	FR	DE	IT	NL	PL	HU	ES	EL
					data) is liable to imprisonment for up to **five** years. - Anyone who **creates, obtains, transfers or allows access to hardware or software adapted to commit cybercrime**, including computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network, is liable to imprisonment for up to **three** years. - **Unsolicited penetration testing:** fine (up to PLN 1.08 million), restriction of liberty or imprisonment for up to two years			
Criminal cases – Who can **request** the use of special investigative techniques	Law Enforcement purposes - requested by public prosecutor or investigative judge	President of the Federal Criminal Police Office or public prosecutor	the public prosecutor	public prosecutor to submit a written request asking for a written prior authorisation	investigative authority	Public prosecutor's office	Public Prosecution services	investigative authority
Criminal cases – Who can **authorise** the use of special	the liberty and custody judge (juge des libertés et de la détention) if requested by the public prosecutor.	Judge (court)	Judge	The investigative judge	local district court	Judge	Judge - has 24 h to respond	Prosecutor of the court of appeal or a judicial council for more serious crimes

	FR	DE	IT	NL	PL	HU	ES	EL
investigative techniques	Otherwise the investigative judge							
Criminal cases – which offenses are covered?	Offences falling within the scope of Articles 706-73 and 706-73-1 of the code of criminal procedure.	Criminal cases considered relevant for Telecom Surveillance (100a STGB): • Crimes of peace treason, high treason and endangering the democratic constitutional state as well as treason and endangering external security ; • Corruption and bribery of elected officials; • Offenses against national defence • criminal offenses against public order; • Counterfeiting money and stamps; • Offenses against sexual self-determination; •Distribution, acquisition and possession of child and youth pornographic content; •Murder and manslaughter; •Offenses against personal liberty; •Gang theft; •Crimes of robbery and extortion; •Commercial stolen goods, gang stolen	The crimes include crimes for which the penalty is over four years' imprisonment, crimes related to drugs, weapons and explosives, as well as smuggling, pedo-pornography, selling fraudulent foods, counterfeit goods, fraud and sale of fraudulent goods, persecution, and involvement on organised crime (associazione di tipo mafioso). In addition, crimes using the telephone as an object are also covered.	Any offence which warrants pre-trial detention. This includes all crimes for which the prison sentence imposed is over 4 years, Further crimes include breaking and entering, squatting, hacking, wiretapping, participation in an organised criminal group, the use of recurring discriminatory or insulting language, illegal disposal of a body, paedophilia, grooming and child pornography, violation of secret, use of violence, fraud, destruction of property (and data), hijacking of ships or planes, money-laundering.	Almost all crimes - Evidence may not be considered inadmissible solely on the grounds of the fact that it has been obtained in violation of the rules of procedure or by means of a prohibited act referred to in Article 1(1) of the Criminal Code, unless the evidence has been obtained in connection with the performance by a public official of his/her personal duties with regard to a murder, wilful injury or deprivation of liberty	The surveillance of private citizens can only be carried out with judicial approval. In matters of terrorism, however, the Police Act refers to the investigatory surveillance mentioned in the National Security Act. Under this provision, judicial approval does not have to be sought to approve the use of these techniques Instead the Minister of Justice is responsible for providing the authorisation.	Suspension of some rights for individuals subjected to investigations of the activities of armed bands or terrorist groups. It does however require "necessary participation of the courts and proper parliamentary control" .	Organised crimes, counterfeiting, human trafficking, rape and sexual abuse of a minor, child pornography) are explicitly mentioned as crimes warranting special investigative techniques. Corruption investigations are also included and covered by a separate article of the code of criminal procedure

	FR	DE	IT	NL	PL	HU	ES	EL
		goods and commercial gang stolen goods; •Money laundering; •Fraud and computer fraud; •Subsidy fraud; •Sports betting fraud and manipulation of professional sports competitions; •Withholding and embezzlement of wages; •Criminal offenses of document forgery; •Bankruptcy; •Criminal offenses against competition; •Criminal offenses dangerous to the public; •Corruption and bribery.						
export of dual-use technologies must be authorised by	*Commission interministérielle des biens à double usage* (Cibdu) covered by national defence secret and therefore not public.	Federal Office for Economic Affairs and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle)	Ministry of Foreign Affairs and International Cooperation National Authority – UAMA (Unit for the Authorizations of Armament Materials)	Ministry for Foreign Affairs (Directorate-General for International Relations - Department for Trade Policy and Economic Governance)	Ministry of Entrepreneurship and Technology Department for Trade in Strategic Goods and Technical Safety	Government Office of the Capital City Budapest Department of Trade, Defence Industry, Export Control and Precious Metal Assay Export Control Unit	the General Secretariat for Foreign Trade (Secretaría General de Comercio Exterior), the Customs Department (Agencia Tributaria - Aduanas) and the Foreign Office Ministry (Ministerio de Asuntos Exteriores, Unión Europea y Cooperación) are the authorities empowered to grant licences and to decide to prohibit the transit of dual-use items	The Ministry of foreign affairs is responsible for authorising the export of dual-use goods (General Secretariat of International Economic Relations and Openness).

	FR	DE	IT	NL	PL	HU	ES	EL
Security services	- Directorate General of Interior Security (Ministry of Interior) - Directorate General of External Security (Ministry of the Armed Forces) - Directorate of Intelligence and Security of Defence (Ministry of the Armed Forces) - National Directorate of the Intelligence and Customs Investigations (Ministry of Economics and Finance)	There are 19 intelligence services, the most important are: - **Federal Intelligence Service (Bundesnachrichtendienst – BND)** (foreign and military - chancellor's office) - **Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz - BfV)**: domestic, ministry of the interior, - **Military Counterintelligence Service (Militärischer Abschirmdienst - MAD)**: military	- Agenzia Informazioni e Sicurezza Esterna (AISE), - Agenzia Informazioni e Sicurezza Interna (AISI)	**- General Intelligence and Security Service** (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) domestic, foreign and signals intelligence, protecting national security (Ministry of the Interior). - **Dutch Military Intelligence and Security Service**	- Internal Security Agency - Intelligence Agency (foreign threats) - Central Anti-corruption Bureau	National Security Service: - Information Office (Prime Minister's office) - the Constitution Protection Office (Minister of the Interior) - Military National Security Service (Ministry of Defence) - Counter-Terrorism Information and Criminal Analysis Centre - Special Service for National Security: assistance for other security services to gather intelligence.	**- National Intelligence Service** (Centro Nacional de Inteligencia, CNI (internal / external) **- Intelligence Center for Counter-Terrorism and Organized Crime** (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, CITCO), (domestic); - **Spanish Armed Forces Intelligence Center** (Centro de Inteligencia de las Fuerzas Armadas, CIFAS)	• The National Intelligence Service (Ethnikí Ypiresía Pliroforión – EYP) – which is the country's national intelligence agency subject to the authority of the Prime Minister (following a change of law in 2019) and is responsible for both foreign and domestic intelligence gathering. • The Hellenic Police Intelligence Division (Διεύθυνσης Διαχείρισης και Ανάλυσης Πληροφοριών - HPiD) constitutes an independent central service acting as a central point for intelligence in the Hellenic Police. It is the intelligence Hub of the Hellenic Police, focusing on combating all forms of crime, but mainly Serious and Organised Crime and Terrorism.
Exceptions for security services	- Loi renseignement 2015 and 2021 regulates duration, severity of the threat, prime ministerial authorisation, etc	Since 2021 all **intelligence services can use state trojans**	Can do surveillance and hacking to achieve their aims	The decision is taken on the basis of a proportionality assessment and both the request by the public prosecutor and the authorisation decision of the	Procedures as simial to criminal cases, with a specific court in charge of authorising the use of special investigative techniques	- No need for judicial authorisation? - Special investigative techniques require the prior authorisation from a judge, the Minister of Justice, or	CNI is authorised by law to carry out "security investigations" without specifying the mechanism or the limits of such investigations	For intelligence services, the process is similar to criminal cases, although the judicial order must have been issued by the Public Prosecutor of the Court of Appeal,

	FR	DE	IT	NL	PL	HU	ES	EL
				investigative judge must be motivated on this basis. The Explanatory Memorandum of the law further requires the Central Review Commission (Centrale Toetsingscommissie) to provide advice to the investigative judge before it takes its decision.		the general directors of the National Security Services		specially assigned to the EYP, who supervises the EYP and controls the legality of its special operational activities as set out in art. 5 of Law 3649/2008
Oversight: Ex-ante	**- Commission nationale de contrôle des techniques de renseignement (CNCTR) :** - mixed control committee - access and legal check - non-binding opinions, annual report = no enforcement mechanism **- Commission nationale de l'informatique et des libertés (CNIL)** **- Défenseur des droits** (Ombudsman)	- Criminal procedure code and law on the police: only be **ordered by the Court at the request of the Public prosecutor's office** **-** if imminent danger: public prosecutor office; falls if not confirmed by the court within three working days - 3 months max + 3	Spyware can be used with specific guarantees (Trojan di Stato): only org crime, only by LEAs, specific place, logged, data security	- **Secret services** can intercept with prior approval of the Minister responsible + authorisation of Investigatory Powers Commission. - In cases where a lawyer or a journalist is targeted, the additional oversight of a court is necessary, with the **District court of the Hague** being responsible for granting **permission** **Three-pronged authorisation:** 1 - internal controls - investigators to convince their internal jurists of the validity of the need for the use of	**- Sejm and Sejm Committee on Security Services** - **Supreme Audit Office** – exercises oversight of the services within the scope of responsibilities of the Office. **- Commissioner for Human Rights** over complaints **- State government bodies (Prime Minister, Minister** – Coordinator of Security Services, Government Council on Security Services) - **Courts and prosecutors** – supervise the conduct of secret surveillance and other surveillance	- Parliamentary Committee on National Security: can request info - procedural guarantees: judicial authorisation by Budapest Metropolitan Court and Minister of Justice	- CNI is under the executive control of the Delegated Committee for Intelligence Affairs - Parliamentary oversight is exercised by the Defence Committee of the Congress of Deputies - CNI shall ask a Magistrate of the Supreme Court for authorisation to intercept communications on the grounds of a threat to the territorial integrity of Spain or the stability of the rule of law	-• The Special Standing Committee for Institutions and Transparency – a parliamentary committee in charge of overseeing policies; administration and management; and the legitimacy of the activities of the EYP. The committee oversees the National Intelligence Service

	FR	DE	IT	NL	PL	HU	ES	EL
				the special investigative technique 2 - seek the approval of the Minister in charge of the services (Ministry of Defence or of the Interior) 3 - Investigatory Powers Commission (Toetsingscommissie inzet bevoegdheden - TIB), whose role is to assess the legality of the approval. The TIB's decision is binding. The TIB is composed of two judges and one technical expert.	operations by security services. **- The Internal Oversight Bureau of the Ministry of the Interior and Administration** supervises the secret surveillance operations carried out by the Police, the Border Guard and the State Protection Service.			
Oversight: Ex-post	**Commission nationale de contrôle des techniques de renseignement (CNCTR)** *See above*	The activities of the BKA and the German intelligence services are subject to judicial control and the technical and legal supervision of the government departments responsible for them (such as the Federal Chancellery, the Federal Ministry of Interior, the Federal Ministry of Defence). For the parliamentary control of the Federal Intelligence Service (BND) there is also the Parliamentary Control	Parliamentary Committee for the Security of the Republic (*Comitato parlamentare per la sicurezza della Repubblica* - COPASIR)	For LEAs: - Inspection of Public Order and Safety (*Inspectie Openbare Orde en Veiligheid)* - Obligation for LEAs to notify the target of surveillance For the intelligence agencies: - Review Committee on the Intelligence and Security Services: access, check legality of actions	**- Minister of Interior** annual (general) **report to the Polish Parliament**	- right to lodge a complaint with the Minister in charge - if dissatisfied, complaint to the National Security Committee of the Hungarian Parliament - complaint to the Ombudsperson, inquiry, can start criminal proceedings or involve the - National Authority for Data Protection and Freedom of Information: only recommendations	- Defensor del Pueblo / Ombudsman can make inquiries on police activities - but not CNI's - **Official Secrets Committee** of the Spanish Congress (officially the Commission for the Control of Credits Allocated to Reserved Expenditures: competent on CNI	• The Authority for Communication Security and Privacy (ADAE) – which is non-parliamentary committee designated by Parliament and appointed by the Minister of Justice, Transparency and Human Rights overseeing the EYP, the Hellenic police and the State Security Division. • The Hellenic Data Protection Authority (HDPA). An independent Authority not subjected to any administrative control. It pertains and answers

	FR	DE	IT	NL	PL	HU	ES	EL
		Committee of the Bundestag						to the Minister of Justice for budgetary purposes.

REFERENCES

- Access Info, Alegaciones al Anteproyecto de la Ley de Información Clasificada, August 2022, available at: https://www.access-info.org/wp-content/uploads/2022-08-12-Access-Info-Alegaciones-Ley-de-Informacion-Clasificada.pdf
- Altalex, Trojan di stato, le novità della legge di conversione sul DL intercettazioni, February 2020, available at: https://www.altalex.com/documents/news/2020/02/28/trojan-di-stato-novita-intercettazioni
- Amnesty International, " Pegasus-Enthüllungen: Amnesty fordert überfällige Regulierung von Spähsoftware" (18.07.2022), available at: https://www.amnesty.de/allgemein/pressemitteilung/pegasus-enthuellungen-amnesty-fordert-regulierung-von-spaehsoftware
- Balkan Insight: Data Dealing: Oversight Concerns in Hungary over AI Data https://balkaninsight.com/2022/01/25/data-dealing-oversight-concerns-in-hungary-over-ai-data/
- Bauer, S. and Bromley, M. 2016. The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World. Non-Proliferation Papers by the EU Non-Proliferation Consortium. No. 48.
- BBC News, "Dutch gangster case: Shock at murder of lawyer Derk Wiersum" (18.09.2019), available at: https://www.bbc.com/news/world-europe-49740366
- Besluit technische hulpmiddelen strafvordering, available here: http://wetten.overheid.nl/BWBR0020444/2013-03-15
- Biermann, Kai, in Die Zeit, "BKA hat NSO-Spähtrojaner bereits mehrfach eingesetzt" (07.09.2021) available at: https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel
- Bits of Freedom, Dutch Senate votes in favour of dragnet surveillance powers, July 2017, available at: https://www.bitsoffreedom.nl/2017/07/12/dutch-senate-votes-in-favor-of-dragnet-surveillance-powers/
- Bodnar, Adam et. al. (2019): How to saddle Pegasus: Observance of civil rights in the activities of security services: objectives of the reform.
- Centre for Democracy and Technology. 2011. 'Going Dark' Versus a 'Golden Age for Surveillance'.
- Citizen Lab, CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru, April 2022, available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
- CitizenLab, HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
- CitizenLab, Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus, July 2021, available at: https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/
- Citizen Lab, UK Government Officials Infected with Pegasus, April 2022, available at: https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/

- Council of Europe. 2016. Venice Commission Opinion, Poland: On the Act of 15 January 2016 Amending the Police Act and Certain Other Acts. Opinion No. 839/ 2016
- Dambrine, B. 2015. The State of French Surveillance Law. Future of Privacy White Paper. 22 December 2015.
- Defensor del Pueblo, El Defensor del Pueblo verifica que la actuación del CNI se ha realizado conforme a la Constitución y la Ley en los casos examinados, May 2022 ? available at: https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/
- Deutscher Journalistenverband, "DJV fordert Aufklärung über Spähsoftware Pegasus" (19.07.2021), available at: https://www.djv-bawue.de/2021/07/19/djv-fordert-aufkl%C3%A4rung-%C3%BCber-sp%C3%A4hsoftware-pegasus/
- Direkt36, Hungarian journalists and critics of Orbán were targeted with Pegasus, a powerful Israeli cyberweapon, available at: https://www.direkt36.hu/en/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele and

  https://telex.hu/direkt36/2021/07/23/az-orban-kormany-allamtitkarat-is-megceloztak-a-pegasusszal-mikozben-belharcokat-vivott-paks-ii-miatt
- Direkt36, The inside story of how Pegasus was brought to Hungary, September 2022, available at: https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/
- EDPS, Preliminary Remarks on Modern Spyware, February 2022, available at: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en
- EDRi, Dutch Parliament: Safety net for democratic freedoms or sleepnet? , available at: https://edri.org/our-work/dutch-parliament-safety-net-democratic-freedoms-sleepnet/ or Amnesty International: Netherlands: End dangerous mass surveillance policing experiments, available at: https://www.amnesty.org/en/latest/press-release/2020/09/netherlands-end-mass-surveillance-predictive-policing/
- Ekimdzhiev and Others v. Bulgaria, Application no. 70078/12, judgement of 11 January 2022, available at: https://hudoc.echr.coe.int/fre?i=001-214673
- El Nacional, Spain's CNI admits spying on Aragonès and on Puigdemont's circle, with court approval https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html
- EPRS, Europe's PegasusGate – countering spyware abuse, July 2022.
- Equipment Interference DRAFT Code of Practice, Autumn 2016.
- Euronews. "Poland's Kaczynski admits country bought Pegasus but denies spying on opponents", (10.01.2022) available at: https://www.euronews.com/2022/01/07/poland-s-kaczynski-admits-country-bought-pegasus-but-denies-spying-on-opponents
- European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017.
- European Parliament. 2015. Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens. P8_TA(2015)0388.

- Florina Cristiana Matei, Andrés de Castro García & Carolyn C. Halladay (2018), On Balance: Intelligence Democratization in Post-Franco Spain, International Journal of Intelligence and CounterIntelligence, 31:4, 769-804, DOI: 10.1080/08850607.2018.1466588 p.776, available at: https://doi.org/10.1080/08850607.2018.1466588
- Forbidden Stories website, available at: https://forbiddenstories.org/case/the-pegasus-project/
- FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, Hungary (2014).
- FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, Greece, October 2014, and EP PEG committee Hearing on 'Use of spyware in Greece', see: https://www.europarl.europa.eu/committees/en/pega-hearing-on-use-of-spyware-in-greece/product-details/20220912CHE10601
- FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, July 2016.
- FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary, 2014.
- FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary, legal update, 2016.
- FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, Poland. Legal update, 2016.
- FranceInfo TV, Projet Pegasus : l'enquête française sur le logiciel espion confiée à un juge d'instruction, July 2022, available at:, https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/projet-pegasus-l-enquete-francaise-sur-le-logiciel-espion-confiee-a-un-juge-d-instruction_5233438.html
- Freedom House, Freedom of the Net 2022, Hungary, available at: https://freedomhouse.org/country/hungary/freedom-net/2022
- Friedman, B. and Kerr, O. Common Interpretation: The Fourth Amendment IV. Available at: https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv
- Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten(Bundeskriminalamtgesetz – BKAG, 01. Juni 2017, p. 76, available at: https://www.bka.de/SharedDocs/Downloads/DE/DasBKA/Auftrag/bkag/bkaGesetz.pdf?__blob=publicationFile&v=1
- Gesetz zur Anpassung des Verfassungsschutzrechts, Federal Law Gazette 2021 Part I No. 40, issued on July 8th, 2021, p. 2274.
- Gill, Peter. 2003. Democratic and Parliamentary Accountability of Intelligence Services after September 11th. Geneva, January 2003. Geneva Centre for the Democratic Control of the Armed Forces. Working Paper No. 103, quoted in Geneva Centre for the Democratic Control of Armed Forces, Intelligence practice and democratic oversight – a practitioner's view, July 2003
- Haaretz news, "Pegasus Spyware Maker NSO Has 22 Clients in the European Union. And It's Not Alone" (09.08.2022), available at: https://www.haaretz.com/israel-news/security-aviation/2022-08-

09/ty-article/.premium/israeli-spyware-maker-nso-has-22-customers-in-12-eu-countries-and-its-not-alone/00000182-8403-df1d-a3a7-ae9bce800000

- Haaretz, As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer Is Building a New Empire, 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
- Haaretz, Criminal Allegations Against Israeli-linked Spyware, Ex-intel Commander in Greek Hacking Scandal, October 2022, available at: https://www.haaretz.com/israel-news/security-aviation/2022-10-07/ty-article/.premium/criminal-allegations-against-israeli-linked-spyware-ex-intel-commander-in-hacking-scandal/00000183-ad14-d3f8-a9ef-bf5752e60000
- Haartez, The Pegasus Project | Where Netanyahu Went, NSO Followed: How Israel Pushed Cyberweapon Sales, July 2021, available at: https://www.haaretz.com/israel-news/tech-news/2021-07-20/ty-article/.highlight/where-bibi-went-nso-followed-how-israel-pushed-cyberweapons-sales/0000017f-e388-d7b2-a77f-e38fd45a0000
- HCLU, Pegasus case: Hungarian procedures, available at: https://hclu.hu/en/pegasus-case-hungarian-procedures
- Hourdeaux, Jérôme, Mediapart, Commerce des armes numériques : la grande hypocrisie , 21 July 2021, available at : https://www.mediapart.fr/journal/international/210721/commerce-des-armes-numeriques-la-grande-hypocrisie
- Hungarian Civil Liberties Union (HCLU), Communication under Rule 9.2 of the Rules of the Committee of Ministers regarding the supervision of the execution of judgments and terms of friendly settlements by the Hungarian Civil Liberties Union, January 2022
- Iefimerida, Σαρωτικές αλλαγές στην ΕΥΠ: Η ΠΝΠ με τις ρυθμίσεις που ενισχύουν τη διαφάνεια -Με 2 υπογραφές εισαγγελέων οι παρακολουθήσεις, August, 2022, available at: https://www.iefimerida.gr/politiki/sarotikes-allages-stin-eyp-praxi-nomothetikoy-periehomenoy
- Immenkamp, B (European Parliamentary Research Service). 2017. Review of dual-use export controls: European Parliament Briefing: EU Legislation in Progress. Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf .
- Including: Michał Kołodziejczak, a farmer and leader of the social movement Agrounia; Adam Hofman, former PiS spokesman; Dawid Jackiewicz, former PiS Treasury Minister in the Cabinet of Beata Szydło; Mariusz Antoni Kamiński, former PiS MP; Bartłomiej Misiewicz, former head of the PiS cabinet and former spokesman of the Ministry of National Defence; Katarzyna Kaczmarek, wife of Tomasz Kaczmarek, former policeman and former CBA officer, later a PiS MP.
- Inside Story, Violation of the legislative process for amendments in law 4790/2021 , March 2021, available at: https://insidestory.gr/article/who-was-tracking-mobile-phone-journalist-thanasis-koukakis
- IRPI media, Cy4gate: the Italian surveillance company seeking to challenge NSO and Palantir, December 2021, available at: https://irpimedia.irpi.eu/en-surveillances-cy4gate/
- Israeli Ministry of Foreign Affairs, Israel MoD tightens control of cyber exports, December 2021, available at: https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021

- Judgment of the Court (Grand Chamber) of 6 October 2020 in Joined Cases C-511/18, C-512/18 and C-520/18, available at: https://curia.europa.eu/juris/liste.jsf?num=C-511/18&language=en
- Kathimerini, PASOK chief files complaint over alleged phone tap attempt, August 2022, available at: https://www.ekathimerini.com/news/1189916/pasok-chief-files-complaint-over-alleged-phone-tap-attempt/
- Kathimerini, Wiretapping case triggers political unrest, August 2022, available at: https://www.ekathimerini.com/news/1190674/wiretapping-case-triggers-political-unrest/
- Korff, D., Wagner, B., Powles, J., Avila, R. and Bürmeyer, U. (2017) Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes. Global Report – January 2017. Available at SSRN: https://ssrn.com/abstract=2894490
- La Moncola, president's news, Pedro Sánchez announces a reform of the legal control regulation of the National Intelligence Centre (CNI) to strengthen its guarantees, May 2022, available at: https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx
- Liberty Human Rights. Article 8 Right to a private and family life. Available at: https://www.liberty-human-rights.org.uk/human-rights/what-are-human-rights/human-rights-act/article-8-right-private-and-family-life .
- Lighthouse Reports, Revealing Europe's NSO, August 2022, available at: https://www.lighthousereports.nl/investigation/revealing-europes-nso/ .
- Ligue de Droits de l'Homme, Loi renseignement 2 : refuser l'emballement sécuritaire, June 2021, availalbe at : https://www.ldh-france.org/loi-renseignement-2-refuser-lemballement-securitaire/
- Marczak, B. et al. 2015. Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. Munk School of Global Affairs.
- Mediapart, « Projet Pegasus » : Mediapart a été espionné par le Maroc, 19 July 2021, https://www.mediapart.fr/journal/international/190721/projet-pegasus-mediapart-ete-espionne-par-le-maroc
- Mediapart, Pegasus : Pedro Sánchez espionné, la confusion politique gagne l'Espagne, May 2022, available at : https://www.mediapart.fr/journal/international/020522/pegasus-pedro-sanchez-espionne-la-confusion-politique-gagne-l-espagne
- Mediapart, Pegasus : une enquête ouverte à Paris, le début d'un long chemin devant la justice, July 2021, available at : https://www.mediapart.fr/journal/international/200721/pegasus-une-enquete-ouverte-paris-le-debut-d-un-long-chemin-devant-la-justice
- Mediapart, Pegasus : vers un nouveau front judiciaire pour les indépendantistes catalans, April 2022, available at : https://www.mediapart.fr/journal/international/250422/pegasus-vers-un-nouveau-front-judiciaire-pour-les-independantistes-catalans
- Memorie van Toelichting Wet Computercriminaliteit III, 2015, Section 2.6.
- Modderkolk, Huib, in de Volkskrant, "AIVD gebruikt omstreden Israëlische hacksoftware" (02.06.2022), available at: https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/

- Moody, G. 2017. Italy Proposes Astonishingly Sensible Rules to Regulate Government Hacking Using Trojans: https://www.techdirt.com/articles/20170216/03431236726/italy-proposes-astonishingly-sensible-rules-to-regulate-government-hacking-using-trojans.shtml.
- Netzpolitik, Pegasus scandal in Hungary: „Not surprising, but still shameful", February 2022, available at: https://netzpolitik.org/2022/pegasus-scandal-in-hungary-not-surprising-but-still-shameful/
- NPR, A spying scandal and the fate of Western Sahara, May 2022, available at: https://www.npr.org/2022/05/11/1098368201/a-spying-scandal-and-the-fate-of-western-sahara
- Ombudsman, 'Apel RPO do Prezydenta w sprawie ustawy antyterrorystycznej' (21 June 2016) https://www.rpo.gov.pl/pl/content/apel-rpo-do-prezydenta-wsprawie-ustawy-antyterrorystycznej
- OMCT, Spain: State surveillance on journalists, politicians, and lawyers, May 2022.
- Omnibus Crime Control and Safe Streets Act (1968), P.L. 90-351, 801, 82 Stat. 197, 212 – provides the US government with procedural regulations surrounding the interception of real-time telecommunications.
- Pietrosanti, F. and Aterno, S. 2017. Italy unveils a legal proposal to regulate government hacking: http://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html.
- Poland, Act on anti-terrorist actions (Ustawa o działaniach antyterrorystycznych), 10 June 2016, Article 9.
- Poland, Act on the Police (Ustawa o policji), 6 September 1990, Article 19.16
- Poland, Poland, Act on Internal Security Agency and Intelligence Agency (Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu), 24 May 2002
- Police Act 1997. C. 50 Part III Authorisation of Action in Respect of Property.
- Polishnews. "Pegasus in Poland. Former judge of the Constitutional Tribunal, Wojciech Hermeliński, on the Senate committee: this could have had an impact on the election result" (26.01.2022), available at: https://polishnews.co.uk/pegasus-in-poland-former-judge-of-the-constitutional-tribunal-wojciech-hermelinski-on-the-senate-committee-this-could-have-had-an-impact-on-the-election-result/
- Politico. "Polish leader under fire over Pegasus hack scandal", (18.01.2022) available at: https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/
- Portolano Cavallo, European Union adopts new regulation no. 2021/821 on dual use, 2021, available at: https://portolano.it/en/newsletter/portolano-cavallo-inform-compliance/european-union-adopts-new-regulation-no-2021821-on-dual-use.
- Privacy International, Italy's Supreme Court decision limits hacking powers and applies safeguards, November 2018 available at: https://privacyinternational.org/news-analysis/2423/italys-supreme-court-decision-limits-hacking-powers-and-applies-safeguards
- Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)

- Reporters without Borders. 2012. The Enemies of Internet, Special Edition: Surveillance. Available at: http://surveillance.rsf.org/en/hacking-team/ .
- Reuters, U.S. State Department phones hacked with Israeli company spyware – sources, December 2021, available at: https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/
- Safety for Sea news item: https://safety4sea.com/union-of-greek-shipowners-provides-10-high-speed-vessels-to-hellenic-cg/
- Mediapart, « Projet Pegasus » : Emmanuel Macron a été ciblé par le Maroc, 20 July 2020, https://www.mediapart.fr/journal/france/200721/projet-pegasus-emmanuel-macron-ete-cible-par-le-maroc
- Security Week, Dutch Used Pegasus Spyware on Most-Wanted Criminal: Report, June 2022? Available at: https://www.securityweek.com/dutch-used-pegasus-spyware-most-wanted-criminal-report
- Sieber, U. and von zur Mühlen. 2016. Access to Telecommunication Data in Criminal Justice: A Comparative Analysis of European Legal Orders. Duncker & Humblot, Berlin, pp. 441-442.
- Simmons and Simmons, Pioneering Dutch Computer Crime Act III entered into force, March 2019.
- Start, Holger, in Die Zeit, "Bundesnachrichtendienst setzt umstrittene Cyberwaffe ein" (08.10.2021), available at: https://www.zeit.de/politik/deutschland/2021-10/pegasus-spionage-software-bnd-kaeufer-einsatz-israel
- Süddeutsche Zeitung. "Bundeskriminalamt verwendet "Pegasus" (07.09.2021), available at: https://www.sueddeutsche.de/politik/cybersicherheit-bundeskriminalamt-verwendet-pegasus-1.5404002
- Tagesschau, Kontrollrat soll Abhöraktionen überwachen, available at: https://www.tagesschau.de/inland/bnd-353.html
- Tagesschau. " Das BKA und die umstrittene Spionage-Software" (07.09.2021), available at: https://www.tagesschau.de/multimedia/video/video-915103.html
- The Guardian, Phone of top Catalan politician 'targeted by government-grade spyware', July 2020, available at: https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware
- The Guardian, FBI confirms it obtained NSO's Pegasus spyware, February 2022, available at: https://www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware
- The Guardian, NSO Pegasus spyware can no longer target UK phone numbers, October 2021, available at: https://www.theguardian.com/world/2021/oct/08/nso-pegasus-spyware-can-no-longer-target-uk-phone-numbers
- The Record, Hungarian official confirms government bought and used Pegasus spyware, November 2021, available at: https://therecord.media/hungarian-official-confirms-governments-bought-and-used-pegasus-spyware/
- The Register, Uncle Sam to clip wings of Pegasus-like spyware – sorry, 'intrusion software' – with proposed export controls, October 201, available at: https://www.theregister.com/2021/10/20/us_intrusion_software_rules/

- The Times of Israel, After NSO bombshell, Gantz asserts that Israel complies with international law, July 2021, available at: https://www.timesofisrael.com/after-nso-bombshell-gantz-asserts-that-israel-complies-with-international-law/
- The Times of Israel, Amid NSO scandal, Israel said to ban cyber tech sales to 65 countries, November 2021, available at: https://www.timesofisrael.com/amid-nso-scandal-israel-said-to-ban-cyber-tech-sales-to-65-countries/
- Thompson, R.M. (2016). Digital Searches and Seizures: Overview of the Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service
- UN Human Rights Council. 2015. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32.
- US Department of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, November 2021, available at: https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list
- Vaciago, G. and Silva Ramalho, D. 2016. Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. Article. Digital Evidence and Electronic Signature Law Review, 13(2016), and Citizen Lab. 2014. Mapping Hacking Team's "Untraceable" Spyware.: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.
- Walker, Shaun, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', The Guardian, 24 January 2022, available at: https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony
- Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017), articles 32-37, available at: https://wetten.overheid.nl/BWBR0039896/2022-05-01
- Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017, available at: https://wetten.overheid.nl/BWBR0039896/2022-05-01
- Wroński, Paweł; Tynkowski, Marcin (7 February 2022). "Cyberatak na Najwyższą Izbę Kontroli. "Mamy podejrzenie włamania Pegasusem na trzy telefony"" [Cyber attack on the Supreme Audit Office. "We have a suspicion of a Pegasus hacking on three phones"]. Gazeta Wyborcza (in Polish). Available at: https://wyborcza.pl/7,75398,28081346,cyberatak-na-najwyzsza-izbe-kontroli-dzis-poznamy-szczegoly.html?disableRedirects=true

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), provides a description of the legal framework (including oversight and redress mechanisms) governing the use of Pegasus and equivalent spyware in a selection of Member States.

PE 740.151
IP/C/PEGA/IC/2022-083

Print ISBN 978-92-848-0005-6 | doi: 10.2861/627219 | QA-04-22-261-EN-C
PDF ISBN 978-92-848-0004-9 | doi: 10.2861/431782 | QA-04-22-261-EN-N