EXECUTIVE SUMMARY

Study for the PEGA committee

European Parliament

The use of Pegasus and equivalent surveillance spyware [1]

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 study, requested by the European Parliament **Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware** (PEGA), **focuses on surveillance spyware like Pegasus, Predator and other equivalent softwares** and analyses the **legal frameworks on surveillance of the countries examined (Greece, Spain, Hungary, Poland, Germany, France, Italy and The Netherlands), as well as their respective oversight and redress mechanisms** (and specifically mechanisms for ex-ante oversight and ex-post santions and remedies). It presents the **European human rights framework on surveillance** that States are bound to respect, before issuing **conclusions and recommendations**. The study also contains a **comparative table** allowing for a cross-cutting comparison of Member States' legal frameworks (see Annex 8).

Key findings

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**.

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 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

[1] Full study in English: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf

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

SR 1274649 EN

Police Office (BKA). In other cases, such as **Greece**, investigative journalists claim that the Predator spyware has been used by the authorities and notably by the intelligence service, while authorities 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 has been denounced by critics as **abusive use of Pegasus and 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 could also be open to criticism.

The glaring gap identified in this report is notably 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, politicians, civil society or private organisations. Effective ex-post oversight mechanisms should have uncovered them and ensure appropriate and effective individual and collective redress mechanisms to bring justice for the victims and ensure that 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. Based on these considerations, **the study concludes that the regular deployment of Pegasus or similar spyware is not compatible with the EU legal order**.

Recommendations

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').

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 as to ensure that these laws respect Article 2 TEU values and notably democracy, the rule of law and fundamental rights.

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.

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.

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.

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.

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.

External Authors:
Quentin LIGER and Mirja GUTHEIL, Asterisk Research and Analysis GmbH

Research Administrator responsible: Ottavio MARZOCCHI Editorial assistant: Sybille PECSTEEN de BUYTSWERVE
Contact: poldep-citizens@europarl.europa.eu

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

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

Print ISBN 978-92-848-0340-8 | doi: 10.2861/549743 | QA-09-23-125-EN-C
PDF ISBN 978-92-848-0337-8 | doi: 10.2861/59767 | QA-09-23-125-EN-N