EXECUTIVE SUMMARY

Study for the PEGA Committee

European Parliament

The impact of Pegasus on fundamental rights and democratic processes [1]

ABSTRACT

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

Background

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

Aim

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

Impact on rights and democracy

Pervasive surveillance affects people's privacy, data protection, and further individual rights - such as the rights to freedom of speech, association, and assembly - as well as the democratic institutions of society. Political participation is affected by spyware in that spied-on citizens can feel compelled to abstain from engaging in interactions having political content, from sincerely expressing their views, and from associating with others for political purposes. This impinges on the quality of a democratic public sphere, which ultimately relies on citizens' input and reactions. More specifically, spyware affects individuals (like journalists, politicians, and activists) who play a special role in the public sphere. Surveillance of such individuals opens space for repression, manipulation, blackmailing, falsification, and defamation. The electoral process itself may be

[1] Full study in English: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

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

SR 1270231EN

influenced, where the collected information, possibly manipulated, is used to carry out smear campaigns against targeted candidates or to engage in other actions affecting their chances of success in the elections. The mere fear of being spied on may induce people to refrain from running for office or from running an effective campaign.

Spyware and national security

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

International human rights law

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

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

EU law

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

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

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

Recommendations

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

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

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

We suggest various strategies that may help prevent abuses:

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

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

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

External Authors: Prof. Dr Giovanni SARTOR, University of Bologna and European University Institute
Prof. Dr Andrea LOREGGIA, University of Brescia
Research Administrator responsible: Mariusz MACIEJEWSKI Editorial assistant: Ivona KLECAN
Contact: poldep-citizens@europarl.europa.eu

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

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

Print ISBN 978-92-848-0550-1 | doi: 10.2861/883809 | QA-04-23-457-EN-C
PDF ISBN 978-92-848-0546-4 | doi: 10.2861/421373 | QA-04-23-457-EN-N