15 February 2022

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Preliminary Remarks on Modern Spyware

Contents

1. Introduction

The revelations made about the Pegasus spyware raised very serious questions about the possible impact of modern spyware tools on fundamental rights, and particularly on the rights to privacy and data protection. This paper aims to contribute to the ongoing assessment in the EU and globally of the **unprecedented risks** posed by this type of surveillance technology. It comes from the EDPS' conviction that the use of Pegasus might lead to an **unprecedented level of intrusiveness**, which threatens the **essence of the right to privacy**, as the spyware is able to interfere with the most intimate aspects of our daily lives.

The distribution and use of spyware tools has been a long-standing serious concern for the EDPS, on which he issued Opinion 8/2015 on the dissemination and use of intrusive surveillance technologies. He underlined that "*[t]he use and dissemination (including inside the EU) of surveillance and interception tools, and related services, should be subject to appropriate regulation, taking into account the potential risk for the violation of fundamental rights, in particular the rights of privacy and data protection*".

As the specific technical characteristics of spyware tools like Pegasus make the control over their use very difficult, we have to **rethink the entire existing system of safeguards** established to protect our fundamental rights and freedoms, which are endangered by these tools.

2. What is Pegasus and how does it work?

According to media reports[1], Pegasus is **probably the most powerful hacking tool** – or spyware – to date. It was developed and marketed around the world by the Israeli company NSO Group. Pegasus is designed to successfully attack almost any smartphone running either iOS or Android operating systems, based on specific information of the target such as the mobile phone number. It can secretly turn a mobile phone into a 24-hour surveillance device, as it gains complete access to all sensors and information of the phone. It can read, send or receive messages that are supposed to be end-to-end encrypted, download stored photos, and hear and record voice/video calls. It has full access to the phone's camera, meaning that it might secretly use it to film you or your environment, or activate the microphone to record real world conversations (for instance, those of people next to you). It also has full access to the geolocation module of the phone, which means it knows where a phone is now and it might also record the timeline of its location.

Pegasus belongs to a new category of spyware tools that differ from "traditional" interception tools used by law enforcement authorities, in a number of ways:

First, it grants **complete, unrestricted access** to the targeted device. According to the research conducted by Amnesty International's Security Lab, this spyware allows the attacker to obtain so-called root privileges, or administrative privileges, on the device: "Pegasus can do more than what the owner of the device can do"[2]. In light of these unprecedented capabilities, one cannot exclude the possibility of using Pegasus beyond mere interception of communications. For instance, it might allow the attacker to gain access to digital credentials or digital identity apps[3], which could be used to **impersonate the victim** and gain access to digital and physical assets, or other similar activities[4].

Second, Pegasus is able to carry out a successful **"zero-click" attack**: a hacking attack that does not require any action by the user to be triggered, so that even a cyber-security-savvy user can do nothing in order to prevent it from happening. Moreover, even the biggest device vendors such as

---

[1] *D. Pegg & S.Cutler, What is Pegasus spyware and how does it hack phones, The Guardian, 2021. Accessed 14 February 2022. https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones*

[2] *Amnesty International, Forensic Methodology Report: How to catch NSO Group's Pegasus, 2021, Accessed 14 February 2022. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/*

[3] *See e.g. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final).*

[4] *Although not yet the case, one can even imagine a next generation of spyware, based on the full and unrestricted control over the target's device, where the attacker moves from 'passive' to 'active' attack, e.g. by 'planting' evidence of crime.*

Apple and Google might not be able to entirely protect individuals from state-of-the-art malware such as Pegasus, despite their constant efforts to enhance the security of their software. Private hacking companies such as NSO Group may have the financial power to contract highly capable software engineers with the sole task of seeking ever-existing vulnerabilities and developing powerful exploits, on par with nation-state capabilities[5].

In addition, Pegasus software is **very difficult to detect** and the intrusions are very hard to prove unless the operating system is powered by secure system logging mechanisms[6]. Security researchers suspect that recent versions of Pegasus inhabit only the phone's temporary memory, rather than its hard drive, meaning that once the phone is powered down virtually, all trace of the software vanishes[7]. Furthermore, the uptake of cloud computing has enabled private companies selling malware and spyware to install their attack infrastructure in the cloud, using highly sophisticated network architectures and application software. Thus, they can provide a hacking service without the need for the customer to install a specific tool, e.g. through offering access to the victim's device via a website. This means that the actual hacking software is always protected[8] and can be always kept up to date and improved for all users, while offering the provider the opportunity to keep control of the tool and of customers.

Pegasus as a "game changer" for digital surveillance

Pegasus should not be equated to "traditional" law enforcement interception tools; instead, it appears to be more similar to "government Trojan" or "online searches" solutions[9] that had in the past raised serious legal concerns, often at constitutional level[10].

Spyware tools like Pegasus are actually hacking tools, and not just means for (lawful) interception of communication. They are based on breaching security mechanisms and exploiting unpatched

---

[5] *L.H. Newman, Google Warns That NSO Hacking Is On Par With Elite Nation-State Spies, The Wired, 2021, Accessed 14 February 2022. https://www.wired.com/story/nso-group-forcedentry-pegasus-spyware-analysis/*

[6] *This is why the security researchers were able to prove the infection of iPhones, as they had sufficient logging mechanisms, which was not the case for Android phones. However a next version of Pegasus might improve in that regard, taking their 'lessons-learnt'.*

[7] *D. Pegg & S.Cutler, What is Pegasus spyware and how does it hack phones, The Guardian, 2021. Accessed 14 February 2022. https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones*

[8] *Amnesty International, Forensic Methodology Report: How to catch NSO Group's Pegasus, 2021, Accessed 14 February 2022. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/*

[9] *For more information see https://www.techtarget.com/searchsecurity/definition/government-Trojan*

[10] *E.g. GFF Challenge to use of government spyware (Germany), Privacy International, 2021, Accessed 14 February 2022. https://privacyinternational.org/legal-action/gff-challenge-use-government-spyware-germany*

vulnerabilities and, in this sense, allowing their use even under strict conditions would create a permanent and strong risk of massive security breaches for all users, comparable in a way with encryption backdoors[11].

Due to its unique features, the Pegasus spyware constitutes a ”game-changer”, combining a level of intrusiveness that is incomparable with what we have seen before, with features capable to render many of the existing legal and technical safeguards ineffective and meaningless. At the same time, it should be borne in mind that Pegasus is not the only spyware tool of this type currently available and the digital market offers a plethora of spyware tools that are often promoted as “law enforcement tools”[12].

3. How can spyware like Pegasus be abused?

NSO Group claims that their technologies “have helped prevent terror attacks, gun violence, car explosions and suicide bombings. The technologies are also being used every day to break up paedophilia, sex- and drug-trafficking rings, locate missing and kidnapped children” as part of the company’s “life-saving mission”[13].

However, the worldwide media investigations indicate another, much **darker side of the software.** There is a growing body of evidence that some of the “vetted customers” applied Pegasus to hack mobile phones and spy on journalists, lawyers, opposition leaders and human rights activists[14].

It has been reported that the **Pegasus spyware had been used in the EU against EU citizens, including opposition politicians, journalists and lawyers.** Some EU governments admitted to

---

[11] In this regard, the CJEU ruled in DRI case that the risk of unlawful access to [telecommunication] data was, in the light of Articles 7, 8 and 52(1) of the Charter, one of the grounds for invalidating Directive 2006/24 (Data Retention Directive), Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Others, paragraphs 54 and 55.

[12] See for example: https://www.softwaresuggest.com/us/pegasus/alternativesor .:

[13] The Pegasus Project, Response from NSO and governments, The Guardian, 2021. Accessed 14 February 2022, https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments. See also: A. Krishna Tal, Phonespy surveillance software mimics Pegasus and was spotted stealing data from thousands of South Korean Android users, Notebookcheck.net, 2021. https://www.notebookcheck.net/Phonespy-surveillance-software-mimics-Pegasus-and-was-spotted-stealing-data-from-thousands-of-South-Korean-Android-users.578637.0.html.

[14] Examples include an alleged use of Pegasus to prepare the assassination of the Saudi journalist Jamal Khashoggi by agents of the Saudi state, see: P. Rueckert, Pegasus. The new global weapon for silencing journalists, Forbidden Stories, 2021. Accessed 14 February 2022, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

having bought Pegasus from the NSO Group[15]. The list of potential customers in the EU may prove even bigger, as it appears that a number of other Members States have at least initiated negotiations with NSO Group for the licencing of the product[16].

Applicable legal framework

Targeted surveillance, including intercepting communications, is regulated in the national legislation of virtually all EU Member States[17]. When it is used for law enforcement purposes, targeted surveillance has to comply with applicable Union primary and secondary law, in particular the Charter of Fundamental Rights[18], the ePrivacy Directive[19] and the Law Enforcement Directive[20].

The legal conditions and safeguards for the use digital surveillance and communication interception have been subject to extensive analysis and interpretation by both the **Court of Justice of the European Union**[21] and the European Court on Human Rights[22]. In particular, in the judgment in Joined Cases C-511/18 and C512/18 (La Quadrature du Net and Others) the CJEU clarified the applicability of EU law to certain measures adopted on national security grounds, namely where obligations are imposed on service providers.

It is important to emphasise that the use of digital surveillance tools by EU Member State authorities for national security purposes, even when it falls outside the scope of Union law[23], is nevertheless subject to national constitutional law as well as the **relevant legal framework of the Council of Europe, in particular the European Convention on Human Rights**[24]**.** In addition, the Convention for the Protection of Individuals with regard to Automatic Processing of

---

[15] Hungary admits to using NSO Group's Pegasus spyware, Deutsche Welle, 2021. Accessed 14 February 2022. https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217 and Z. Wanat, Poland's Watergate: Ruling party leader admits country has Pegasus hacking software, Politico, 2021. Accessed 14 February 2022. https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/

[16] D. Leloup & M. Untersinger, Malgré les approches de NSO Group, la France a choisi à la fin de 2020 de ne pas acheter le logiciel espion Pegasus, Le Monde, 2021. Accessed 14 February 2022. https://www.lemonde.fr/pixels/article/2021/11/26/malgre-les-approches-de-nso-group-la-france-a-choisi-a-la-fin-de-2020-de-ne-pas-acheter-le-logiciel-espion-pegasus_6103783_4408996.html

[17] See Fundamental Rights Agency (FRA) report "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", 2017.

[18] OJ C 326, 26.10.2012, p. 391–407.

[19] OJ L 201, 31.7.2002, p. 37–47.

[20] OJ L 119, 4.5.2016, p. 89–131.

[21] See for example CJEU judgments in joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, case C-623/17, Privacy International, etc.

[22] See e.g. ECtHR judgments in cases Zakharov v. Russia, Big Brother Watch and Others v. the United Kingdom, Ekimdzhiev and Others v. Bulgaria.

[23] Pursuant to Article 4(2) TEU "national security remains the sole responsibility of each Member State".

[24] See CJEU judgment in Joined Cases C-511/18 and C-512/18, La Quadrature du Net and Others, para. 103.

Personal Data (**Convention 108**), recently modernised as Convention 108+, applies to processing of personal data for State (national) security purposes, including defence[25].

4. Can Pegasus be used legally within the scope of EU law?

Pegasus and similar technologies are often advertised as "law enforcement tools". In this regard, it is important to analyse whether it is legally possible to use Pegasus or similar tools in the EU to pursue objectives of general interest recognised by the Union, such as combating terrorism and serious crime.

Terrorism and organised crime pose serious threats within the European Union and globally, and their detection, prevention and prosecution represent important objectives of general interest which may justify limitations on the exercise of the fundamental rights and freedoms of the individual, in accordance **with Article 52(1) of the EU Charter of Fundamental Rights**, to the extent that they are proportionate and necessary**.** Such limitations must in any event be provided for by law and respect the essence of the fundamental rights and freedoms recognised by the Charter.

The CJEU acknowledged in its recent case law[26] that a serious threat to national security that is genuine and present or foreseeable could justify very serious interferences with fundamental rights, subject to strict conditions and safeguards.

Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal[27]. Given the scarcity of publicly available verifiable information about the functionalities of Pegasus, it is difficult to ascertain to what extent its use could not be replaced by the use of other, more "traditional" and potentially less intrusive means.

---

[25] *Article 9 of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) Article 11 of Convention 108+.*
[26] *E.g. Judgment in Joined Cases C-511/18 and C-512/18, La Quadrature du Net and Others.*
[27] *See also the EDPS Necessity Toolkit available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf*

Furthermore, today we all rely on smartphones to perform most of our activities in the digital world. Our smartphones know everything about us: they know our data, they can hear us, they can see us, and they know where we are and who we talk with. It is therefore highly unlikely that spyware such as Pegasus, which de facto grants full unlimited access to personal data, including sensitive data, **could meet the requirements of proportionality**[28].

The level of **interference with the right to privacy is so severe that the individual is in fact deprived of it.** In other words, the essence of the right is affected. Therefore, its use cannot be considered proportionate – irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state[29]. Moreover, it is not just the target of the surveillance whose right to privacy is manifestly infringed, but also everybody in contact with him or her or even those around them (e.g. people sitting a restaurant close to the target could also be recorded). Furthermore, Pegasus and similar spyware deprive the affected individuals of additional forms of protection, such as **confidentiality of communication** with a lawyer.

At the same time, the EDPS takes note of the media reports alleging that certain features of Pegasus might be switched off, in order to limit the intrusiveness of the tool, which might have an impact on the result of the proportionality and necessity assessment. Therefore, one cannot exclude the possibility that the application of certain features of Pegasus may pass the necessity and proportionality test in specific situations of very serious threat, such as **imminent terrorist attack**.

However, the EDPS considers that such cases would be of exceptional nature and cannot justify a wider or systematic deployment of such highly intrusive technology. Consequently, regular deployment of Pegasus or similar highly intrusive spyware technology would not be compatible **with the EU legal order.**

In addition, the capability of spyware tools such as Pegasus to provide full and unrestricted control by the attacker of the target's phone, coupled with the fact that they leave very little, if any, digital traces, raises the question of to what extent the information gathered with their help could be used as evidence in a criminal procedure - from the point of view of both admissibility and verification.

---

[28] *"For a measure to respect the principle of proportionality enshrined in Article 52(1) of the Charter, the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of fundamental rights", see EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019, available at https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf*

[29] *See CJEU judgment in case C-362/14 Maximillian Schrems v Data Protection Commissioner, para. 93–94.*

In this regard, many of the forensic experts may not have the necessary knowledge to identify and examine such highly advanced technology, especially when developed by private companies.

Consequently, one may argue that the use of such advanced hacking tools to collect evidence in a criminal investigation could actually **encroach on the right to fair trial**, provided for in Article 47 of the Charter, which is one of the of the cornerstones of European legal systems.

5. What could and should the EU do?

The recast of the **EU Dual Use Regulation**[30] introduced new export controls for "cyber-surveillance items". Still, the overall protection needs to be strengthened in order to guarantee that cyber-surveillance items will never be exported to countries that do not ensure the respect of fundamental rights, including the right to privacy. Moreover, such controls should also cover import of such dual-use technologies, as much as export. In this context, it should borne in mind that blacklisting of spyware vendors alone is not enough for ensuring the effective application of the Regulation.

The mounting evidence shows that highly advanced military-grade spyware like Pegasus has the potential to cause **unprecedented risks and damages** not only to the fundamental rights and freedoms of the individuals but also to **democracy and the rule of law**. Pegasus constitutes a paradigm shift in terms of access to private communications and devices, which is able to affect the **very essence of our fundamental rights, in particular the right to privacy**. This fact makes its use incompatible with our democratic values.

Therefore, the EDPS believes a **ban on the development and the deployment of spyware with the capability of Pegasus** in the EU would be the most effective option to protect our fundamental rights and freedoms. In any event, if such tools are nevertheless applied in exceptional situations, e.g. to prevent a very serious imminent threat, the EDPS proposes the following non-exhaustive list of **steps and measures as a guarantee against unlawful use**:

[30] *OJ L 206, 11.6.2021, p. 1–461.*

1. **Strengthening of democratic oversight over surveillance measures**. EU Member States should ensure effective oversight over the use of such surveillance measures. The role of data protection authorities, judicial control (ex ante and ex post), and democratic forms of scrutiny are absolutely necessary.[31] Any form of evaluations and monitoring must be meaningful and effective. While there is no 'one-size-fits-all' solution, there is a need for a broad spectrum of actions in a modern checks and balances system. The Commission's annual Rule of Law report should take into account the standards of national legislation in this field.

2. **The strict implementation of the EU legal framework on data protection**, especially the Law Enforcement Directive, is a critical prerequisite. Equally important is the full implementation of the relevant CJEU judgements (e.g. on data retention), which is still lacking in several Member States. In this regard, the Commission as the "guardian of the EU Treaties" pursuant to Article 17 of Treaty on the European Union (TEU)[32], has a central role for enforcing EU law and ensuring its uniform application throughout the Union.

3. **Judicial review, both ex-ante and ex-post, should be real; it cannot be a mere formality.** When reviewing an application for a surveillance order, the judicial authority should always be aware of what kind of surveillance would be carried out (e.g. when highly intrusive monitoring of an individual's activity is foreseen), in order to allow the court to decide whether the surveillance remains within what is strictly necessary.

4. **Strengthening of the protections offered by the criminal procedure.** Criminal procedural laws should outlaw the use of highly intrusive hacking tools like Pegasus. Based on Article 82 of the Treaty on the Functioning of the European Union (TFEU)[33], the EU has the competence to adopt minimal standards on the rights of individuals in criminal procedures. This includes restricting the admissibility of evidence collected with the help of highly intrusive hacking tools like Pegasus or even outlawing it[34]. The EU could also, based on Article 83 TFEU, define criminal offences such us illegal use of spyware technologies.

5. **Reducing the risk that data originating from such undemocratic and abusive surveillance practices reaches the databases of the Union** (e.g. Europol) and Member States law enforcement agencies, e.g. through "import" of criminal intelligence and other data from third countries, circumventing the legal limitations in the Union.

6. **Stop (ab)using national security purposes for legitimising politically motivated surveillance.** "National security" cannot be used as an excuse to an extensive use of such technologies nor as an argument against the involvement of the European Union. Both the jurisprudence of the CJEU and the relevant binding international legal framework, in particular the ECHR and Convention 108 of the Council of Europe, show clear limitations

---

[31] See Fundamental Rights Agency (FRA) report "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", Volume I, Chapter 2. "Oversight of intelligence services", 2017.
[32] OJ C 326, 26.10.2012, p. 47–390.
[33] OJ C 326, 26.10.2012, p. 47–390.
[34] Under the so-called 'fruit of the poisonous tree' doctrine.

that need to be strictly observed by state authorities[35]. The EDPS draws attention to the role the ePrivacy Directive might play in the safeguarding against the level of intrusions which modern spyware creates.

7. **Addressing the rule of law problems**. Deficiencies in the rule of law and democratic backsliding, such as encroaching on judicial independence or media freedom, create fertile ground for abuse of secret surveillance, with tools like Pegasus. Therefore, such issues within the EU should be addressed and enforced as a matter of priority.

8. **Empowering civil society to bring awareness and public debate forward**. Only with strong civil society, can democratic control can be exercised over the use of surveillance measures by the State. Abuse of such tools against politicians, journalists and activists has many times been discovered thanks to civil society. It is our duty to support it.

With this document, the EDPS would like to contribute to the discussion on whether spyware tools like Pegasus should have any place in a democratic society. At the centre of any such discussion, should not only be the use of the technology itself, but the importance we attribute, as a society, to the right to privacy as a core element of human dignity.

[35] *See the EDPB response to MEP István Ujhelyi on the alleged use of the Pegasus spyware, available at https://edpb.europa.eu/system/files/2021-12/edpb_letter_out_2021-00160_mep_ujhelyi.pdf, and also https://hungarytoday.hu/pegasus-hungary-spyware-data-authority-naih-peterfalvi/*