European Parliament
LIBE Committee exchange of views on Pegasus spyware

November 29th 2021 | to be organised between 15:45-16:45 - hybrid meeting

Purpose of event

Following the revelations made about the Pegasus spyware[1], Members of the LIBE Committee would like to hear from you about **your assessment on the issues raised by such program and its consequence for fundamental rights, and particularly its impact on privacy**. This would be highly relevant to the LIBE Members, in their continuous work on fundamental rights.

A **timeslot of 7 min is foreseen per speaker to present your statement/analysis, followed by Q&A session with the Members**.

[1] See e.g. https://en.wikipedia.org/wiki/Pegasus_(spyware), https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ or https://www.theguardian.com/news/series/pegasus-project.

Participants:

To cover all the elements of this case, the LIBE Committee has also invited two other speakers to this exchange of views with LIBE Members: a representative of the Forbidden Stories consortium and a technical expert from Amnesty International's security lab.

- **Forbidden Stories** is a consortium of journalists whose mission is to continue the investigations of murdered, imprisoned or threatened journalists.
- **Amnesty International** is a global movement of more than 10 million people who take injustice personally. "*We are campaigning for a world where human rights are enjoyed by all*".
- **The Security Lab of Amnesty International**, launched in 2019 and located in Berlin, leads technical investigations into cyber-attacks against civil society and provides critical support when individuals face such attacks. The Lab also builds tools and services to help protect human rights defenders from cyber-attacks, and conducts technical training with the wider support community to help them identify and respond to digital threats.

Suggested speaking points:

- Thank for this invitation and also thank you for the opportunity to exchange views on a very important subject which has already drawn my attention due to **specific aspects related to the right to the protection of personal data**.

- The use of targeted digital surveillance tools **clearly interferes with the fundamental rights to privacy and protection of personal data in the EU** and it may adversely affect other fundamental freedoms, such as the freedom of thought and religion, freedom of expression and information, or freedom of assembly and of association.

- We all rely on smartphones to perform our activities in the digital world, now more than ever. Our **smartphones know everything about us**: they know our data, they can hear us, they can see us, they know where we are with whom we talk.

- If such spyware tools are available on the market, this means that **anyone who has the power and the money to purchase such spyware tools** can have **full access to our lives**, not just our data, which automatically constitutes **a serious violation** of our privacy and our rights and freedoms.

- I have noted with the utmost concern the reporting that the Pegasus spyware had also been used in the EU against EU citizens, including Hungarian journalists. We have all read in the past months in the

digital media that some EU governments admitted having bought Pegasus from the NSO Group, which further supports that the allegations were real.

- We all know that these tools exploit vulnerabilities of operating systems and other software. I would like to make it clear that it is the **responsibility of the software providers** to guarantee the security of their products in an accountable way, by promptly doing security tests, addressing discovered vulnerabilities and applying immediately the proper patches plus the appropriate information of the public. This will ensure also **compliance with data protection and cybersecurity regulations**.

- Apart from vulnerability management, those providers could improve the security of their products by using as much as possible **open source code, which has major advantages for security and transparency**. I would also suggest introducing integrity checking mechanisms as well as advanced system logging which can become of critical importance for the investigation of such cases.

- The distribution and use of spywares is a long-standing serious concern, on which the EDPS has notably issued an opinion back in 2015, **opinion 8/2015 on the dissemination and use of intrusive surveillance technologies**, after the revelations about the activities of the **Italian HackingTeam**. Amongst our recommendations then to the European and national legislators was that "*The 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***".

- I remember very well that at that time, the then European Data Protection Supervisor, Giovanni Buttarelli, stated in a public alert that "*As the unregulated market for the trading and use of covert monitoring technology continues to grow, the EU must not underestimate the appetite for such technology. By addressing weaknesses in existing legislation and policies as well as developing new legislation, the EU legislator can help protect against the very real threat posed to our privacy and data protection rights. The sale of these privacy-invasive dual-use tools and the offer of related services also needs to be more tightly regulated in the EU to prevent human rights abuses in Europe and further afield.*".

- **I realize that these warnings have not yet received a satisfactory response, after 6 years**. The use of such technologies is still not sufficiently regulated and this is the main reason **we are discussing this issue today again**. **Blacklisting of spyware vendors is not enough**.

- **Even without a specific regulation in place**, to the extent it would fall within the scope of Union law, any deployment of these tools by Member States' authorities would need to meet **the tests of necessity, proportionality, and legitimate objectives** as outlined

under the EU legislation on confidentiality of electronic communication (ePrivacy Directive 2002/58/EC) and personal data protection (GDPR) and/or Law Enforcement Directive.

- As you very well know, the EDPS is the independent authority of the European Union (EU) responsible for the supervision of the processing of personal data by Union institutions, offices, bodies and agencies. This means that **I do not have the competence to investigate the specific cases at hand**.

- However, the EDPS is a **permanent member of the EDPB**, which has the competence to deal with these issues at Member State level, to the extent it would fall within the scope of Union law. Consequently, the EDPS is and will remain actively involved in all EDPB discussions and work relating to spywares.

- Thank you again for this opportunity to discuss with you this important topic.

Analysis of the allegations and technology used

> ➢ A very good **visual description of how pegasus works** in this video by The Guardian.

Both of the participating organisations played a **leading role** in **revealing governments' espionage** on journalists, opposition politicians, activists, business people and others using the private **Pegasus spyware** developed by the Israeli technology and cyber arms firm NSO Group.

- On 2/10/2018, **Jamal Khashoggi**, a Saudi Arabian journalist, dissident, author, columnist for The Washington Post, and a general manager and editor-in-chief of Al-Arab News Channel, **was assassinated** at the Saudi consulate in Istanbul on 2 October 2018 by agents of the Saudi government. While the investigation mostly points to Khashoggi's close associates being targeted in the months after the murder, it also identified evidence suggesting that an NSO client targeted the phone of his wife, Hanan Elatr, several months before his death, between November 2017 and April 2018. The client appears to have used NSO's spyware, Pegasus, which **can transform a phone into a surveillance device, with microphones and cameras activated without a user knowing**.

- In 2020, **a target list of 50,000 phone numbers** leaked to **Forbidden Stories**, and an analysis revealed the list contained the numbers of leading opposition politicians, human rights activists, journalists, lawyers and other political dissidents. From this list it was revealed that **also Hungarian journalists, businesspeople and an opposition politician were targeted**. Recently the Hungarian government admitted that it had bought the military-grade spyware Pegasus, produced by Israel-based NSO Group.

- More than half of these phones were **inspected by Amnesty International's cybersecurity team** which revealed forensic evidence of the Pegasus spyware, a **zero-click Trojan virus** developed by NSO Group. This malware provides the attacker **full access to the targeted smartphone, its data, images, photographs and conversations as well as camera, microphone and geolocation**.

- On 18/7/2021 **Amnesty has published Forensic Methodology Report**: How to catch NSO Group's Pegasus in which it is shown **how the spyware works**. The methodology was validated by an independent Canadian IT security laboratory.

- NSO had found certain vulnerabilities in the iOS software (mainly in iMessage and iTunes) from which it could deliver 'zero-click' attacks in the iPhone. 'Zero-click' means that **the attack was carried out without the user of the device to click on a link or even to open an attachment or even to open an application**. The operating system itself was infected by malicious messages sent in the iMessage of the victim.

- NSO has established **a highly sophisticated infrastructure** in order to deliver the attacks to the victim devices, comprised of "URL Shortener Servers", "Pegasus Installation Servers", and "Installation DNS Servers". NSO Group's Pegasus infrastructure primarily consists of **servers hosted at datacentres located in European countries** (including OVH, this was also revealed by this article Giant Datacenter Fire Takes Down Government Hacking Infrastructure!). The countries hosting the most infection domain DNS servers included Germany, the United Kingdom, Switzerland, France, and the United States (US).

- Much of the targeting outlined in this report involves Pegasus attacks targeting iOS devices. It is important to note that this does not necessarily reflect the relative security of iOS devices compared to Android devices, or other operating systems and phone manufacturers. **The reason why iOS devices seem to be the target is because the forensic analysis found log files in those phones, which do not exist in android phones**!

- Amnesty International **strongly encourages device vendors to explore options to make their devices more auditable, without of course sacrificing any security and privacy protections already in place**. The also recommend platform developers and phone manufacturers to regularly engage in **conversations with civil society to better understand the challenges faced by HRDs**, who are often under-represented in cybersecurity debates.

- This information was passed along to 17 media organisations under **"The Pegasus Project"** umbrella name, **under the coordination of Forbidden Stories**. **Reports started to be published by member organisations on 18 July 2021, revealing notable non-criminal targets and analysing the practice as a threat to freedom of the press, freedom of speech, dissidents and democratic opposition**. On 20 July, 14 heads of state were revealed as former targets of Pegasus malware. Various parties called for further investigation of the abuses and a limitation on trading such repressive malware, among them the newsrooms involved, the Committee to Protect Journalists, the International Press Institute, and Edward Snowden.

- On 6/10/2021, on digital news: another case of use of Pegasus spyware, Dubai ruler hacked ex-wife using NSO Pegasus spyware, high court judge finds.
- On **14/10/2021**, the Pegasus Project was awarded the 2021 Daphne Caruana Galizia Prize for Journalism **by the European Parliament**. The winning story was the article Pegasus: The new global weapon for silencing journalists • Forbidden Stories.
- Likewise in October 2021, it was made public that also the **German Federal Police Office (Bundeskriminalamt)** had bought a version of the Pegasus spyware and had made use of it since March 2021, albeit in a modified version to bring it in line with German law.[2]
- On **3/11/2021** it became public that the Biden administration blacklists NSO Group over Pegasus spyware.
- On 23/11/2021 Apple announced in its website that **it sues NSO Group to curb the abuse of state-sponsored spyware**. In the same article, **Apple also announced a $10 million contribution to support cybersurveillance researchers and advocates** (like the Security Lab of Amnesty International).
- On digital news 24/11/2021: France allegedly negotiated with Israeli-owned NSO group to buy its Pegasus spying software, according to the MIT Technology Review. Talks reportedly broke down after revelations in July identified Emmanuel Macron as one of the software's many targets.

[2] https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-smartphone-103.html

Background on EDPS and EDPB cases relevant to the Pegasus spyware

EDPS

EDPS Case 2021-0770: **On 31 August 2021**, the EDPS **sent a reply to Mr István Ujhelyi**, Member of European Parliament, Vice-Chair of the Committee on, Transport and Tourism (following a letter from the MEP to the EDPS on 10 August 2021, regarding the use of the spyware Pegasus) with the following **main points**:

- **I have noted with the utmost concern** the reporting that the Pegasus spyware **was used against Hungarian journalists** ('the Pegasus Case').
- The use of targeted digital surveillance tools clearly **interferes with the fundamental rights to privacy and protection of personal data in the EU and it may adversely affect freedom of expression**. The distribution and use of spywares is a long-standing serious concern, on which the EDPS has notably issued an opinion (European Data Protection Supervisor, Opinion 8/2015 on the dissemination and use of intrusive surveillance technologies) and a corresponding alert.
- At that time, the EDPS had recalled that '[T]he processing of personal data within the scope of EU law by **the competent authorities for law enforcement purposes should also respect the standards and safeguards laid down in the EU Charter of Fundament Rights**. Article 7 of the Charter enshrines the right of privacy, for which the protection of personal data can be of fundamental importance. Thus **the intrusion into the virtual domicile through spyware, exploits, or similar devices, should be considered a violation of one's privacy'**.
- As the **EDPS** is the independent authority of the European Union (EU) responsible for the supervision of the processing of personal data by EU institutions and bodies, it **does not have the competence to investigate the**

specific case that you have brought to my attention, regardless its possible merits.

- However, I **appreciate** that several MEPs have already addressed parliamentary questions on 20 July 2021 to the Commission inquiring, among other things, whether the Commission will investigate a possible breach of the EU Treaties, the Charter of Fundamental Rights of the EU, the General Data Protection Regulation ('GDPR') and the Law Enforcement Directive. In this respect, you may be aware that the Commission reportedly announced on 20 July 2021 that it is gathering information on the Pegasus Case.
- I take due note of your request to discuss the matter at the level of the European Data Protection Board ('EDPB'). **I consider the matter to be of the utmost importance and I will therefore recommend to the EDPB Chair to have the issue of spywares addressed in one of the next EDPB plenary meetings**.

The full reply of EDPS is attached here. 

The LTT on that case was the following:

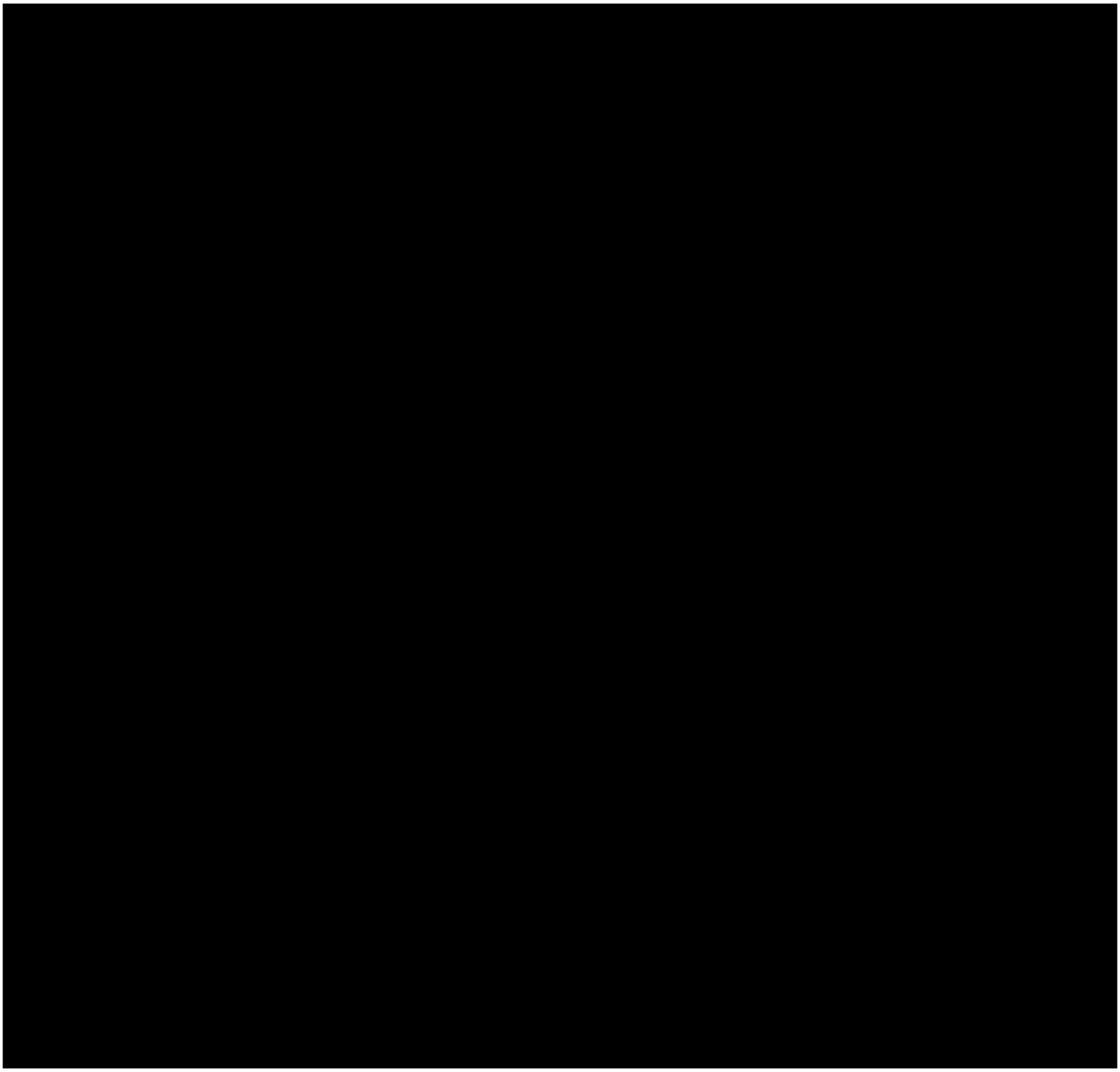
- The EDPS is deeply concerned about the alleged massive targeting of human rights activists, journalists and lawyers across the world by authoritarian governments using hacking software sold by the surveillance company NSO Group;

- Commonly these tools exploit vulnerabilities of operating systems and other software. Software providers are responsible for guaranteeing that any detected vulnerability (whether it is publicly disclosed or directly reported) is promptly addressed and that a patch is made available, to ensure product security and compliance with data protection and IT security regulations;

- In the EU, the use of targeted digital surveillance tools such as Pegasus infringe interferes in particular with the fundamental rights to privacy and protection of personal data and may adversely affect the rights of freedom of expression;

- Any deployment of these tools by Member States' authorities would need to meet the tests of necessity, proportionality, and legitimate objectives as outlined under the EU legislation on confidentiality of electronic communication (ePrivacy Directive 2002/58/EC) and personal data protection (GDPR) and/or Law Enforcement Directive ;

- It would however seem clear from the information in the public domain that the alleged uses of the tool are abusive and arbitrary, and do not constitute a permissible interference with these rights to privacy and personal data protection.



[redacted]

EU Dual-Use Regulation

On 11 June 2021, Regulation 2021/821 was published in the Official Journal of the European Union ('the Regulation'). The Recast Dual-Use Regulation entered into force on 9 September 2021 and replaced the Dual-Use Regulation introduced in 2009.

Key changes include[3]:

- Two new general export authorisations: The Regulation introduces a general export authorisation for intra-group transfers of dual use software and technology to specified countries for product development purposes, that is available where the parent company is resident in an EU Member State or an EU General Export Authorisation 001 destination country, and is subject to conditions including the parent company providing a guarantee for the subsidiary's compliance with the authorisation. A further export authorisation is introduced for certain encryption items, and permits exports to countries other than those on a negative list.

- New requirements for internal compliance policies and due diligence: Whilst some Member States already require exporters to implement an Internal Compliance Programme for export controls in order to obtain global export authorisations, this is now an EU-wide requirement (with limited exceptions).

[3] https://www.politico.eu/article/europe-to-curtail-spyware-exports-to-authoritarian-countries/

https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/

- Technical assistance: The Regulation introduces new controls covering situations where a company provides technical assistance relating to dual-use items. Previously, export controls would not apply to the provision of technical assistance other than where controlled technology (or controlled goods or software) were exported as part of the assistance.

- Cyber-surveillance: **The Regulation introduces a new end-use control on cyber-surveillance equipment, where the exporter is aware or has been informed that the exported items are or may be intended for use in connection with internal repression or the commission of serious violations of human rights and international humanitarian law. This applies to items (whether or not listed) that are specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems.**

- Relationship with national control lists: To address public security concerns and facilitate cooperation between member states to prevent circumvention of national controls, exporters may be required to seek authorisation where items are placed on national control lists in another Member State.

- License duration and record-keeping: Global and individual authorisations will now only be valid for a maximum of two years. Further, records must be kept for five years (as opposed to the current three year period) following the end of the calendar year in which a transfer took place.

Proposed LTT:

- The adoption of Regulation 2021/821 is a step in the right direction given its broader scope compared to the previous regulation on dual-use items.
- In particular, the EDPS welcomes the addition of a definition of 'cyber-surveillance items' and the possibility to subject these items to an authorisation procedure even if they are not explicitly listed in Annex I of the Recast Dual-Use Regulation. This evolution is in line with the recommendations made in the EDPS Opinion 8/2015.
- However, the overall protection still needs to be strengthened, in particular to ensure a clear and consistent identification of the cyber-surveillance items not listed in Annex I of the Recast Dual-Use Regulation (i.e. dual-use items that are not automatically subject to an authorisation procedure). More generally, the EDPS would recommend hardening the authorisation regime in order to guarantee that cyber-surveillance items will never be exported to countries that do not ensure the right to privacy.

- In accordance with Article 42(1) EUDPR, the EDPS expects to be consulted on any amendment to the Recast Dual-Use Regulation having an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.

[redacted]

Case officers / contact points

- [redacted]