

(English version)

**Question for written answer E-001920/24
to the Commission**

Saskia Bricmont (Verts/ALE), Anna Strolenberg (Verts/ALE), Martin Hojsík (Renew), Veronika Cifrová Ostrihoňová (Renew), Ľubica Karvašová (Renew), Michal Wiezik (Renew), Lucia Yar (Renew), Leoluca Orlando (Verts/ALE), Jan Farský (PPE), Jeroen Lenaers (PPE), Jana Toom (Renew), Murielle Laurent (S&D), Gordan Bosanac (Verts/ALE), Krzysztof Brejza (PPE), Gaetano Pedulla' (The Left), Hannah Neumann (Verts/ALE), Emma Rafowicz (S&D), Dario Tamburrano (The Left), Giuseppe Antoci (The Left), Birgit Sippel (S&D), Olivier Chastel (Renew), Krzysztof Śmiszek (S&D), Benoit Cassart (Renew), Merja Kyllönen (The Left), Marie Toussaint (Verts/ALE), Damien Carême (The Left), Sebastian Everding (The Left), Nathalie Loiseau (Renew), Mounir Satouri (Verts/ALE), Rasmus Nordqvist (Verts/ALE), Markéta Gregorová (Verts/ALE), David Cormand (Verts/ALE), Danuše Nerudová (PPE), Ľudovít Ódor (Renew), Raquel García Hermida-Van Der Walle (Renew)

(1 October 2024)

Subject: Use of Pegasus and other types of spyware in Slovakia

According to recent press reports ⁽¹⁾, Slovak intelligence services have acquired Pegasus spyware. This technology targets mobile devices and enables the extraction of very sensitive personal data, as well as being able to activate a device's microphone and camera. In June 2023 Parliament adopted a report ⁽²⁾ calling for strict conditions to be put in place to restrict the use of such intrusive technologies. Given the current situation in the country — including attacks on journalists, activists, civil society, and the opposition — we are very concerned that the potential use of this spyware will pose a significant threat to fundamental rights and the rule of law.

1. Has the Commission contacted the Slovak authorities to confirm the acquisition and use of spyware in Slovakia and to assess the potential implications for democracy and the rule of law?
2. What measures does the Commission intend to take to ensure that surveillance technologies comply with data protection requirements and respect human rights within the EU?
3. We understand that the Commission will be publishing a communication regarding the use of spyware. When will the communication be published and will it include binding obligations for Member States, as recommended by the report from Parliament's PEGA Committee?

Supporter ⁽³⁾

Submitted: 1.10.2024

**Answer given by Mr Reynders on behalf of the European Commission
(28 November 2024)**

The Commission strongly condemns any illegal access to interpersonal communications. Regarding potential implications to the rule of law, the Commission monitors the situation in all Member States, including Slovakia.

The data protection *acquis* offers comprehensive protection to the confidentiality of communications and users' personal data. EU data protection law is applicable to the processing of personal data by private entities, even where such processing is required for national security purposes.

Under the ePrivacy Directive ⁽¹⁾, the interception or surveillance of communications by public or private bodies is prohibited without the consent of the user.

While restrictions to these rights are permitted for important public objectives, they are subject to conditions and safeguards. The Law Enforcement Directive ⁽²⁾ is also applicable when public authorities process personal data for law enforcement purposes. Courts and supervisory authorities have effective powers to examine any allegations of misuse.

Member States are competent to safeguard their national security. They must oversee their security services to ensure they respect fundamental rights.

¹ <https://dennikn.sk/4176198/tajna-sluzba-za-fica-zrejme-ziskala-moznost-totalne-ovladnut-mobil-moze-ist-o-nastroj-pegasus/https://www.article19.org/resources/slovakia-use-of-pegasus-a-threat-to-democracy-and-human-rights/>.

² https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html.

³ This question is supported by a Member other than the authors: Raphaël Glucksmann (S&D)

⁽¹⁾ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

⁽²⁾ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.

The investigation of such issues is the responsibility of each Member State. Member States cannot merely refer to national security to exclude the application of EU law. The Court of Justice of the EU made clear that Member States must be able to demonstrate why national security would be compromised in the case at issue.

As the Commission informed the European Parliament in its answers to the dedicated resolutions, it is working on a non-legislative proposal on the use of intrusive surveillance software by national authorities in the EU, in particular from a data protection perspective.
