

(English version)

**Question for written answer E-002029/25
to the Commission
Nikolaos Anadiotis (NI)
(20 May 2025)**

Subject: Uncontrolled use of spyware — Threat to national sovereignty and fundamental rights

In Greece, there has been unprecedented institutional outrage at the illegal, opaque and unaccountable surveillance of journalists, politicians, judges and state officials through Predator spyware (see ‘Predatorgate’, wiretapping scandal), with no one yet being held responsible ⁽¹⁾.

At the same time, new surveillance platforms, such as Paragon, are circulating widely on the European market, unhindered, uncontrolled and without any unified supervisory framework ⁽²⁾. This constitutes a threat not only to the privacy of European citizens but also to fundamental freedoms and human rights, freedom of the press, the democratic functioning of the Member States and national security.

In light of the above:

1. What further steps does the Commission intend to take with a view to establishing a single and binding European regulatory framework that will strictly control the use of spyware within the EU?
2. Does the Commission intend to establish a mandatory reporting and notification mechanism for the use of spyware by Member States, in order to ensure democratic scrutiny, transparency and compliance with the EU Charter of Fundamental Rights?

Submitted: 21.5.2025

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(1 August 2025)**

The Commission has clearly stated that any attempt to illegally access data of citizens, including journalists and political opponents, if confirmed, is unacceptable and remains fully committed to ensuring that Member States’ actions in this context fully respect the EU Charter of Fundamental Rights.

The European regulatory framework includes several different safeguards to address the use of spyware within the EU.

Firstly, the data protection and privacy *acquis* offers comprehensive protection to the confidentiality of communications and users’ personal data and terminal equipment.

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 without the consent of the user is in principle prohibited. While restrictions are permitted for important public objectives, they are subject to strict conditions and safeguards.

Moreover, the Law Enforcement Directive ⁽²⁾ is also applicable when competent authorities process personal data for law enforcement purposes. Supervisory authorities have effective powers to examine any allegations of misuse, and data processed can be subject to judicial review.

Finally, as regards the protection of journalistic sources and confidential information, the Commission recalls that Article 4(3) (c) of the European Media Freedom Act ⁽³⁾ (EMFA) will become applicable as of 8 August 2025.

¹ <https://balkaninsight.com/2024/08/02/greek-parliament-refuses-to-question-supreme-court-over-spyware-ruling/?utm>

² <https://www.reuters.com/technology/cybersecurity/metasploit-says-israeli-spyware-company-paragon-targeted-scores-users-2025-01-31/?utm>

⁽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.

⁽³⁾ Regulation (EU) 2024/1083: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1083>. The provision stipulates that ‘Member States shall ensure that journalistic sources and confidential communications are effectively protected’ and that, subject to a strictly limited derogation, ‘Member States shall not deploy intrusive surveillance software on any material, digital device, machine or tool used by media service providers, their editorial staff or any persons who, because of their regular or professional relationship with a media service provider or its editorial staff, might have information related to or capable of identifying journalistic sources or confidential communications’.

The application of this and other safeguards in EMFA will ensure free and independent media across the EU and protect them against interference. The Commission will use all tools at its disposal to ensure the effective application of EU law.
