

(English version)

**Priority question for written answer P-002126/26
to the Commission
Alvise Pérez (NI)
(24 May 2026)**

Subject: Surveillance of a Member of the European Parliament by national intelligence services without judicial authorisation

It has come to my attention that the Spanish intelligence services are reportedly monitoring me, a Member of the European Parliament, without authorisation or judicial scrutiny, in both my political activity and my private life. I have photographic evidence of this in my possession.

Article 4(2) of the Treaty on European Union does not exclude EU law from applying when it affects the rights set out in Articles 7, 8 and 11 of the Charter. The intelligence services' activity in relation to citizens, especially political representatives in the performance of their duties, should therefore be subject to independent, preferably judicial, scrutiny of any secret surveillance.

In light of the above,

1. Does the Commission consider monitoring elected officials without prior judicial authorisation to be compatible with the Charter and with the aforementioned standards?
2. What safeguards does the Commission consider necessary, in line with the PEGA Committee's recommendations, against the use of intelligence against political representatives?
3. In the Commission's view, what impact do such practices have on the independence of Parliament and Protocol No 7?

Submitted: 25.5.2026

**Answer given by Mr McGrath on behalf of the European Commission
(12 August 2026)**

The follow-up and investigations into the alleged illegal use of spyware are a responsibility of national authorities. The Commission strongly condemns any illegal access or any form of unlawful interception of users' communications.

EU law on data protection and privacy offers comprehensive protection to the confidentiality of communications and users' personal data and terminal equipment.

Without prejudice to the Commission's role as guardian of the Treaties, the monitoring and enforcement of EU law lies primarily with the competent national authorities and courts.

Member States are required under Directive 2013/40/EU ⁽¹⁾ to ensure that cyberattacks, such as illegal access to information systems, illegal interception and the use of tools to commit such offences are punishable as criminal offences.

The responsibility for the investigation and prosecution of such offences falls under the responsibility of competent national authorities.

The Commission takes the recommendations of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA) seriously.

It also notes that the Venice Commission's report on the regulation of spyware sets out several procedural safeguards that are needed when using spyware for law enforcement purposes ⁽²⁾.

The 2025 Rule of Law Report ⁽³⁾ follows up on developments concerning the alleged illegal use of spyware in the context of the functioning of national checks and balances in response to such allegations. The Commission continues to monitor developments in this area.

⁽¹⁾ <https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng>.

⁽²⁾ Report on a rule of law and human rights compliant regulation of spyware, adopted by the Venice Commission at its 141st Plenary Session (Venice, 6-7 December 2024) — Venice Commission of the Council of Europe <https://www.coe.int/en/web/venice-commission/-/cdl-ad-2024-043-e>.

⁽³⁾ 2025 Rule of Law Report https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/annual-rule-law-cycle/2025-rule-law-report_en.