

(English version)

**Question for written answer E-002375/25
to the Commission
Sandro Gozi (Renew)
(12 June 2025)**

Subject: Paragon scandal

Following the revelations concerning spyware developed by Paragon and used to target the director of Fanpage, it appears that the Italian Government could have rooted out the source of that surveillance, but failed to do so. This case brings the Predator scandal to mind.

The attacks on press freedom, national authorities' failure to respond and the opaque relationship between governments and private providers of surveillance technology highlight the dangers of not having a clear legal framework governing companies such as Paragon. They also raise major questions about regard for the rule of law and fundamental rights safeguarded by the European Union.

With a view to getting accurate information on what happened and who is responsible, is the Commission considering opening a structured dialogue with the Italian authorities?

Submitted: 12.6.2025

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

The 2025 Rule of Law report ⁽¹⁾ referred to the use of Paragon's spyware in Italy, noting the concerns raised by stakeholders, as well as the actions taken by Italian authorities.

These actions include an inquiry carried out by the Parliamentary Committee for the Security of the Republic. In its report, approved unanimously and published in June 2025, the Committee stated that it had not identified any use of the spyware by Italian intelligence services to target Italian journalists.

Nevertheless, it reserved the right to carry out further investigations as appropriate. In parallel, the Italian Government instructed the National Cybersecurity Agency to investigate the case while underlining that it had no knowledge of the matter.

The Commission considers that any attempt to illegally access data of citizens, including journalists and political opponents, if confirmed, is unacceptable, and will continue to monitor and address any developments in this context using the relevant legal framework.

Notably, as of 8 August 2025, Article 4(3)(c) of the European Media Freedom Act ⁽²⁾ (EMFA), focusing on the protection of journalistic sources and confidential information, is applicable.

This and other safeguards, such as the right to effective judicial protection foreseen in Article 4(8), will ensure free and independent media across the EU and protect them against interference.

Moreover, the ePrivacy Directive ⁽³⁾ prohibits the interception of communications and the storage of and access to information in the terminal equipment without the prior consent of the user concerned and any restrictions based on public objectives are subject to strict conditions and safeguards. The Law Enforcement Directive ⁽⁴⁾ is also applicable when competent authorities process personal data for law enforcement purposes.

Finally, once applicable, the Cyber Resilience Act's cybersecurity requirements for market access in the EU of hardware and software will make it more challenging for threat actors to, *inter alia*, deploy spyware.

⁽¹⁾ https://commission.europa.eu/document/download/9ccf6a60-8e2f-4193-868b-30a24c9e37e0_en?filename=16_1_63949_coun_chap_italy_en.pdf.

⁽²⁾ Regulation (EU) 2024/1083: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1083>.

⁽³⁾ Directive 2002/58/EC: <https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng>.

⁽⁴⁾ 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, 4.05.2016.