

**Question for written answer E-003317/2026
to the Commission**
Rule 144
Fabio De Masi (NI)

Subject: Legal accountability and preventive measures for cybersecurity breaches caused by autonomous AI systems

Recent incidents involving highly capable AI systems have demonstrated that autonomous systems may identify and exploit vulnerabilities, access external systems and cause cybersecurity breaches in ways that were not explicitly designed or anticipated by their developers¹²³.

In such circumstances, it appears that European regulation has so far been inadequate in identifying legal responsibilities and preventing such incidents. In this respect, Article 2(8) of Regulation (EU) 2024/1689⁴ excludes from the scope of the AI Act research, testing and development activities concerning AI systems or AI models prior to their being placed on the market or put into service.

In the light of the above, we pose the following questions to the Commission.

1. Do any of the activities involved in the OpenAI and Anthropic incidents, as described above, fall outside the scope of the AI Act under Article 2(8)?
2. What supervisory action has the Commission taken, or what action does it intend to take, in response to these incidents under its existing powers?
3. Does the Commission consider that the existing EU legal framework provides sufficiently clear rules establishing responsibility and liability where an autonomous AI system, during research, testing or development, independently exploits a cybersecurity vulnerability and causes damage to a third party?

Submitted: 24.8.2026

¹ <https://www.bbc.com/news/articles/cz7dl7w8y7po>.

² <https://edition.cnn.com/2026/08/04/tech/ai-anthropic-openai-security-breach-intl-hnk>.

³ <https://www.bbc.com/news/articles/c2el319vzr3o>.

⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).