

Anfrage zur schriftlichen Beantwortung E-003317/2026
an die Kommission
Artikel 144 der Geschäftsordnung
Fabio De Masi (NI)

Betrifft: Rechtliche Rechenschaftspflicht und Präventivmaßnahmen bei Bedrohungen der Cybersicherheit durch autonome KI-Systeme

Jüngste Vorfälle, an denen hochleistungsfähige KI-Systeme beteiligt waren, haben gezeigt, dass autonome Systeme Schwachstellen erkennen und ausnutzen, auf externe Systeme zugreifen und die Cybersicherheit in einer Weise bedrohen können, wie es von ihren Entwicklern weder ausdrücklich konzipiert noch antizipiert wurde.¹²³

Insofern sind die europäischen Rechtsvorschriften anscheinend bislang unzureichend, um die rechtlichen Verantwortlichkeiten zu ermitteln und solche Vorfälle zu verhindern. Was dies betrifft, so sind gemäß Artikel 2 Absatz 8 der Verordnung (EU) 2024/1689⁴ Forschungs-, Test- und Entwicklungsaktivitäten im Zusammenhang mit KI-Systemen oder KI-Modellen vom Anwendungsbereich der Verordnung über künstliche Intelligenz ausgeschlossen, solange diese Systeme oder Modelle noch nicht in Verkehr gebracht oder in Betrieb genommen wurden.

1. Fallen Tätigkeiten im Zusammenhang mit den oben erwähnten Vorfällen von OpenAI und Anthropic gemäß Artikel 2 Absatz 8 nicht in den Anwendungsbereich der Verordnung über künstliche Intelligenz?
2. Welche Aufsichtsmaßnahmen hat die Kommission als Reaktion auf diese Vorfälle im Rahmen ihrer bestehenden Befugnisse ergriffen bzw. welche Maßnahmen gedenkt sie zu ergreifen?
3. Ist die Kommission der Auffassung, dass der bestehende EU-Rechtsrahmen hinreichend klare Vorschriften zur Festlegung von Verantwortung und Haftung enthält, wenn ein autonomes KI-System während der Forschungs-, Erprobungs- oder Entwicklungsphase eine Schwachstelle im Bereich der Cybersicherheit autonom ausnutzt und Dritten Schaden zufügt?

Eingang: 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 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).