

(English version)

**Question for written answer E-001361/26
to the Commission
Raquel García Hermida-Van Der Walle (Renew)
(1 April 2026)**

Subject: Increasing use of and investment in Palantir software

In recent years, law enforcement and intelligence agencies in the EU have increasingly used software produced by the US tech company Palantir, which can analyse very large quantities of data to identify patterns and make predictions about crime. Recent media coverage revealed that investment in Palantir by European banks, asset managers, insurers and pension funds increased by almost 70% from 2024 to 2025 ⁽¹⁾.

Palantir is widely considered to be controversial because of its close connections to the White House and its supply of software to US Immigration and Customs Enforcement (ICE) to help find irregular migrants. The company's CEO recently stated that its technology is intentionally discriminatory and disruptive to our democratic societies ⁽²⁾.

Several Member States currently use Palantir technologies, while Europol used Palantir software between 2016 and 2021 ⁽³⁾.

1. Is any Palantir technology or product currently used by the Commission or by any of its agencies or bodies?
2. Does the Commission agree that the use of Palantir in the EU poses significant risks, not only by threatening fundamental rights but also by essentially giving the United States a way to pressure Member States to act to the White House's liking?
3. As part of its focus on more European digital sovereignty, does the Commission plan to stimulate the development of European alternatives that comply with EU laws and values?

Submitted: 1.4.2026

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(1 July 2026)**

The Commission does not use any Palantir technology or product.

The Commission recalls that the Charter of Fundamental Rights of the EU ⁽¹⁾ applies to EU institutions, bodies and agencies, and to Member States when they implement EU law.

Regarding predictive policing, the AI Act ⁽²⁾ introduces safeguards to protect fundamental rights, including non-discrimination. It prohibits AI systems from assessing or predicting the risk of a person committing a criminal offence based solely on profiling or personality traits and characteristics.

Other AI systems used to assess crime risks are classified as high-risk and are therefore subject to specific requirements and obligations.

The same applies to AI systems used to assess risks in migration, asylum and visa applications, or to detect and identify individuals in migration contexts.

As part of the adopted European technological sovereignty package ⁽³⁾, the Open Source (OS) Strategy ⁽⁴⁾ aims to support open, secure alternatives aligned with EU law and values.

It is expected to put forward measures to help OS communities and EU companies develop, scale up, maintain and secure high-quality OS components, and to accelerate their adoption by public and private actors.

This includes support for existing sovereign alternatives and new solutions in strategic areas where dependencies exist. It will also aim at promoting a voluntary EU assessment framework to recognise solutions that comply with key EU rules and values, while avoiding technological isolation.

¹ <https://www.ftm.eu/articles/european-investors-palantir-investment>.

² <https://newrepublic.com/post/207693/palantir-ceo-karp-disrupting-democratic-power>.

³ <https://www.euractiv.com/news/palantir-is-well-on-its-way-to-conquering-europe/>.

⁽¹⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT>.

⁽²⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>.

⁽³⁾ https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en.

⁽⁴⁾ <https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy>.