

# European Software and Cyber Dependencies

Check out the [original full study](#) by scanning this QR code



Europe's digital ecosystem remains heavily dependent on non-EU software and cloud providers, primarily US firms, creating strategic vulnerabilities. This study maps these dependencies and identifies geopolitical and economic risks and outlines policy options to strengthen EU's technological autonomy and resilience.

This report was prepared for the Policy Department for Transformation, Innovation and Health at the request of the ITRE Committee.

## Software overview



Non-EU actors, primarily US companies, dominant Europe's digital stack, with European offerings confined to niche or complementary positions. Dependencies are reinforced by vendor lock-in, long-term contracts, proprietary formats, and network effects that limit European innovation. Compared to US and China, Europe also lags in software R&D, AI patents, and deep-tech investment, focusing on complementary innovations rather than core platforms. The trend is observed in virtually all segments of software market analysed in the study.

- **Cloud infrastructure:** AWS, Microsoft Azure, and Google Cloud hold about 70% of the EU market. While the overall cloud computing market in the EU has grown significantly in the past decade, the combined share of EU providers has fallen to roughly 13% by 2022<sup>1</sup>. Even EU's largest player, SAP, captures only around 2% of the EU cloud computing market. Given that cloud underpins most modern software, this is a highly strategic dependency;
- **Enterprise software:** Around 80% of EU corporate spending on software and cloud flows to US vendors<sup>2</sup>. Microsoft, Oracle, Salesforce, and IBM dominate productivity, CRM, and analytics tools. SAP is the only prominent European vendor, especially strong in the ERP software market;
- **Consumer platforms:** Android and iOS command virtually 100% of mobile OS usage; Windows holds 73% of desktop OS share, while iOS has most of the rest; Google Search exceeds 89% of web search; US platforms control social media and browsers market almost entirely<sup>3</sup>;
- **Cybersecurity:** US and Israeli vendors dominate tools such as firewalls, identity management, and Security Information and Event Management (SIEM) systems, while EU firms specialise mainly in services (Thales, Atos, Orange Cyberdefense) and specialised OT/ICS niches;
- **Government IT:** Public administrations rely heavily on Microsoft and Google productivity suites and US clouds, with only isolated instances of migrations to open-source alternatives (e.g., LibreOffice, Nextcloud).



## Risks and strategic vulnerabilities

EU's reliance on US tech exposes it to sovereignty risks, as the CLOUD Act and US sanctions allow foreign access to European data — even when stored locally. "Sovereign-cloud" offerings by hyperscalers only partially mitigate these risks, as ownership and legal control remain non-EU, often described as "sovereignty-washing." Software dependencies lock the EU into a situation in which EU firms innovate within ecosystems defined elsewhere, ceding intellectual property, data, and scale advantages to foreign players. This entails major macro-economic costs and erodes Europe's long-term competitiveness:

- The EU's digital trade deficit exceeds EUR 100 billion annually; roughly EUR 264 billion per year (around 1.5% of EU GDP) flows to foreign cloud and software vendors<sup>4</sup>;
- Retaining just 15% of these outflows could create around 500,000 jobs in Europe by 2035<sup>5</sup>;
- Lock-in inflates long-term costs and undermines innovation, while dependence on external platforms diminishes Europe's leverage in trade and security negotiations;
- Productivity growth lags behind the US: if EU's digital-sector productivity matched US levels, total EU productivity would rise by around 1.2%<sup>6</sup>.

## European options

The EU retains strong assets that can be mobilised to rebuild technological sovereignty. Several broad strategic pillars emerge in the study:

- **Sovereign cloud and AI:** scaling federated, EU-controlled infrastructure, while investing in AI "factories" and data centres under EU jurisdiction;
- **Open-source and digital commons:** treating open source as strategic infrastructure, funding critical projects and ensuring sustainable governance;
- **Industrial alliances and PPPs:** using partnerships to pool R&D, setting open standards, and fostering cross-sector collaboration, including for dual-use defence applications;
- **Regulatory and procurement levers:** simplifying and enforcing the digital acquis; requiring open standards, multisourcing, and "Buy European" clauses in public IT procurement; restoring sovereignty criteria in cloud certification;
- **Research, skills, and global cooperation:** boosting technology and AI R&D funding, developing EU-wide digital-skills pipelines, and deepening collaboration with like-minded countries.

<sup>1</sup> Synergy Research Group, 2022, *European Cloud Providers Continue to Grow but Still Lose Market Share*. Available at: <https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share>

<sup>2</sup> Asterès., 2025, *Technological dependence on American software and cloud services: An assessment of the economic consequences in Europe (Economic Study)*, Cigref. Available at: <https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf>

<sup>3</sup> Statcounter, 2025. *Global Stats*. Available at: <https://gs.statcounter.com/>

<sup>4</sup> Asterès., 2025.

<sup>5</sup> Ibid.

<sup>6</sup> Ibid

**Disclaimer and copyright.** The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2025.

© Image on page 1 used under licence from Adobe Stock.

ECTI/B/ITRE/FWC/2022-108/LOT2; Manuscript completed: December 2025; Date of publication: December 2025 PE 780.413

Administrator responsible: Anne PLOEGER; Editorial assistant: Irene VERNACOTOLA

Contact: [ecti-poldep-b@europarl.europa.eu](mailto:ecti-poldep-b@europarl.europa.eu)

This document is available on internet at: [www.europarl.europa.eu/supporting-analyses](http://www.europarl.europa.eu/supporting-analyses)

Print ISBN 978-92-848-3291-0 | doi: 10.2861/1975677 | QA-01-25-289-EN-C

PDF ISBN 978-92-848-3290-3 | doi: 10.2861/6959336 | QA-01-25-289-EN-N