Sovereignty versus Autonomy: Europe's contradiction of Digital Dependency

29 OCTOBER 2026

Silas van Gorkum

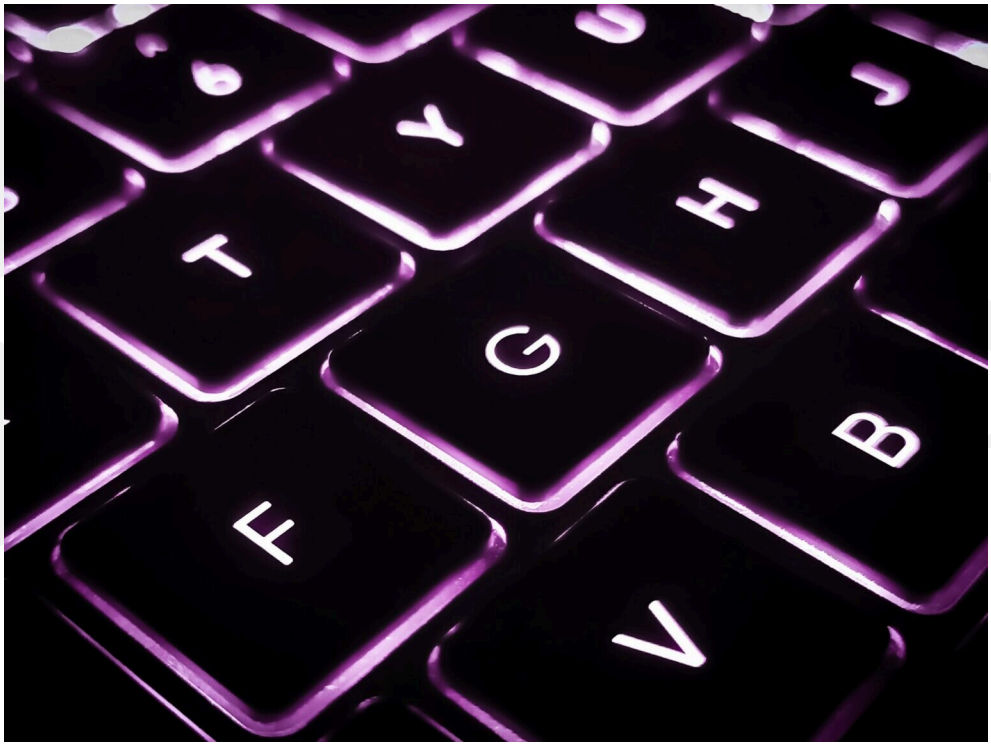


Photo by Protagonist on Unsplash

Introduction

In 2026 the European Commission presented the Tech Sovereignty Package, the latest instrument in a regulatory sequence running from the GDPR (General Data Protection Regulation), NIS2 and the Cybersecurity Act. This continues an unresolved contradiction. The EU has spent two decades building the world's most demanding cybersecurity rulebook, yet Europe is still dependent on foreign providers.

Two forms of sovereignty separate here. Regulatory sovereignty is the authority to set enforceable rules within a jurisdiction. Operational autonomy

is the capacity to keep functioning without a foreign power's cooperation. Edler et al. (2023) define technology sovereignty as the capacity to act, and this article adopts their definition as its single test. The EU advanced on the first while the second stalled.

The contradiction frames the following question: to what extent has regulatory sovereignty over digital infrastructure produced the operational autonomy member states need to exit non-European providers, and which policies widen their ability to do so? Three measures structure the answer: legal exposure to foreign compulsion, supply continuity, and time.

The Scale of Dependency

The European Commission's own numbers are in evidence. The explanatory memorandum for the 2026 Cloud and AI Development Act (CADA) states the collective cloud market share of EU-based providers fell from roughly 29 per cent to about 15 per cent in 2022 (Gundermann, 2026); three US hyperscalers now hold more than 70 per cent of the market (van Klinken, 2026). According to a European Parliament report, digital products, services and infrastructure from non-EU sources are over 80 per cent (Khafo, 2025).

No European hyperscaler matched US providers in price or scope, and years of "Cloud First" procurement that followed defaulted to the platform was already inside the government IT department. A legal mechanism turns this commercial choice into a jurisdictional one. The US CLOUD Act mandates that American firms provide data to US authorities at any time (Cross-Border Data Sharing under the CLOUD Act, 2025). A Microsoft server in Amsterdam puts Europeans at the risk of American law.

Anton Carniaux of Microsoft France testified on 10 June 2025 to a French Senate committee on public procurement and digital sovereignty. When he was asked to guarantee French citizens' data would never reach US authorities without French government consent, he answered under oath: "No, I cannot guarantee it" (CE Commande Publique: Compte Rendu De La Semaine dU 9 Juin 2025, 2025). Microsoft's technical director for the French public sector, Pierre Lagarde, told the same hearing that customer data had been within the EU since a contract in January 2025 (CE Commande Publique: Compte Rendu De La Semaine dU 9 Juin 2025, 2025). Both statements are true, but there is no legal guarantee in a technical arrangement.

Cases of Digital Exposure

The two cases in EU jurisdiction further illustrate the problem: EU law found the digital arrangements unlawful, and resolution still took years.

France centralised the health records of millions of citizens on Microsoft Azure because officials judged no European provider matched the scale (Marchandon, 2026). The 2020 Schrems II ruling struck down the transatlantic Privacy Shield, and France's data protection authority told the Conseil d'État Microsoft's safeguards were deficient, and the hosting was

illegal (McDermott Will & Emery, 2020). The court allowed supervised continuation. The government promised to migrate to a European facility by the end of 2022, and the deadline slipped for years. The Hub moved to Scaleway, a French company, in April 2026 (Marchandon, 2026). Regulation flagged the problem in 2020. Six years passed before a change of provider resolved the problem, and capacity constraints caused the delay.

In November 2022, Germany's federal and state data protection authorities concluded public bodies had no path to compliant use of Microsoft 365 under EU data law without additional safeguards (Lomas, 2022). The European Data Protection Supervisor found in 2024 that the Commission's own use of the software breached EU data protection rules (European Data Protection Supervisor (EDPS), 2024). Microsoft provided the fix. EU Data Boundary build-out was completed in February 2025, Data Protection Addendum was made public in September, and the German state of Hesse became the first state to declare compliant use to be possible (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2025). Almost three years separate the result from the first sign of resolution.

In both cases an EU law identified the problem correctly. The solution came only after a member state put pressure for years and the firm changed its architecture and standards of regulation. Regulation made the exposure undeniable but did not produce the fix.

Regulation Without Capacity

Brussels responds with more regulatory legislation. The GDPR, the NIS2 Directive, the Cybersecurity Act and the 2026 Tech Sovereignty Package form one sequence. The central piece of that is CADA, which separates cloud and AI services into four sovereignty levels. The first tier allows US hyperscalers to operate freely. The top-tier covers about 1% of public sector data and bars providers unless the Commission grants an exception (EUR-Lex, 2026). The Executive Vice-President Henna Virkkunen claims that the European Union wants to ensure that "nobody has a kill switch" over Europe's critical systems (Nicol-Schwarz, 2026).

Farrand and Carrapico (2022) call this regulatory mercantilism. CADA fits that definition. American law requires public buyers to favour domestic suppliers, but CADA has no buy-European mandate, because the Commission was trying to dissuade US retaliation. They create no supplier to deliver to that tier.

Two design choices deepen the gap. Member states administer enforcement so a reasonable national reading allows the hyperscaler to win a sensitive contract. The control test also weighs nominal ownership, that is, who controls the shares, against effective control, or who controls how the system is running. Twenty-four European cloud CEOs under CISPE called this weakness 'sovereignty washing' (Hale, 2026).

The trend of "sovereignty washing" continued in April 2026. The Commission awarded its first sovereignty-scored cloud contract to four European companies under an eight-point Cloud Sovereignty Framework. Three winners are fully EU-owned. Proximus was the fourth, and it included S3NS, a joint venture between Thales and Google Cloud (European Commission, 2026). Legal exposure improved on paper. Supply continuity and time to remedy remained. A rule does not allow a firm to be part of a tier. A rule does not build a firm to fill the tier.

Regulatory Sovereignty and Operational Autonomy: One Framework, Two Layers

Edler et al. (2023) define technology sovereignty as the capacity to act, and this article adopts the definition as its single test.

Three measures worked in this case. Legal exposure to foreign compulsion is mostly in the authority layer. Supply continuity and time to remedy are in the capacity layer. Every case does not pass the test on at least one of these three measures. The Microsoft testimony cannot be viewed as legal exposure, as the contract and contract-bound data boundaries of the CLOUD Act still cover the law and are not in the reach of the CLOUD Act. The Health Data Hub fails on the other two: six years between the 2020 finding and the migration to Scaleway. Microsoft 365 fails to fix it in time: three and a half years between the German finding and the first sign of resolution. Legal exposure and supply continuity in the S3NS bid remain open.

Two layers follow. The authority layer is rule-setting within a jurisdiction, regulatory sovereignty. The capacity layer includes a buyer's freedom to refuse a supplier and keep functioning, which is operational autonomy. Pohle and Thiel (2020) draw a parallel line between control and capacity. Edler et al. warn of near autarky, so autonomy here means managed interdependence. Sensitive workloads need an exit option. General workloads do not.

Farrand and Carrapico (2022) explain why the authority layer is chosen. Rules provide for market position at low fiscal cost. In addition, Bradford (2019) predicts EU rules will change firm behaviour even more globally, and Microsoft's EU Data Boundary and Data Protection Addendum are in line with the prediction. Both changes reduced exposure to GDPR. CLOUD Act exposure, ownership and exit options stayed as before. The EU had an influence over the vendor and still relies on the vendor. The EU cloud share fell from 29 per cent in 2017 to 15 per cent in 2022 (Gundermann, 2026), and the GDPR and the Cybersecurity Act are in place. Scale, price and incumbent-default procurement led to the loss, and regulation did not reverse the trend. The layers move independently, and there is no causal connection in either direction. Regulatory sovereignty has not led to operational autonomy.

What Closing The Gap Would Require

Closing the gap requires building all three measures together. Control rules deal with legal exposure, supply issues about continuity and buyer capacity is related to time to remedy. No measure comes first because each is fed back to the others. The Health Data Hub shows the loop. A number of officials felt there was no European provider of the scale of Azure, so the contract went to the incumbent. European providers remained small without major buyers. Six years passed before the data shifted (Marchandon, 2026). Ownership decides legal exposure. General workloads accept foreign-owned capacity, but those with sensitive tiers require EU oversight. That only works if we have control and EU enforcement in place. CADA has neither. Sovereign-by-construction platforms are somewhere in the middle between the tiers. Each has a domestic operator over foreign technology. France's Bleu, a subsidiary of Orange and Capgemini, will run Microsoft Azure and Microsoft 365 under French ownership (Bleu, 2026). Germany's Delos Cloud, an SAP subsidiary based on Azure, operates under BSI oversight (Bertelsmann, 2024). Nobody has tested whether this structure is effective in removing CLOUD Act exposure when an American firm licenses the technology in question. Neither of the platforms offers supply continuity, so they are transitional. The Dutch government has blocked Kyndryl from buying Solvinity, which hosts DigiD infrastructure. The block protects the legal exposure and does not add any capacity (Haeck, 2026).

Supply is the tightest constraint. Martens (2026) puts EU AI compute at about two gigawatts, or about 5 per cent of the global total, and expects planned projects to move the share little. Speed and grid access have to prohibit supply more than ownership. The Dutch sovereign cloud design shows managed interdependence in practice. The design aims for full software control and gives up hardware dependence (Loohuis, 2026); no European manufacturer ever makes CPUs, GPUs or ASICs.

Demand builds supply over time. In order to do so, procurement increases supplier capacity when buyers work together. Stojčić et al. (2020) find a large impact of procurement on innovation and output of 41,623 firms in 8 Central and Eastern European countries. Some EU member states are starting to take action on these findings. France will replace Microsoft Teams and Zoom with Visio by 2027 across state offices (Davies, 2026). Schleswig-Holstein moved nearly 80 per cent of state workplaces to LibreOffice by the end of 2025 (Krempl, 2025). Where policy has been certified or fined in the past, governments acquire and operate capacity, and other public bodies will reuse the result.

Organisations limit how far this goes. Uyarra et al. (2020) point to a lack of uptake of innovation procurement as being due to poor buyer capability, poor coordination and low incentives. The Dutch municipal platform Signalen has roughly 15 contributing municipalities, versus 30 to 40 needed

for long-term sustainability (Linåker et al., 2026). A public sector with no technical staff cannot consider an exit option, let alone take one.

The improvements are partial. About 20 per cent of workplaces in Schleswig-Holstein still rely on Microsoft because specialised applications are built into Office (Krempl, 2025). Visio restricted meetings to 150 people in April 2026, and Teams to 10,000 people (GARO, 2026). France, Germany and the Netherlands also create separate platforms and work in parallel. This duplication doesn't violate Edler et al.'s warning. (2023) against autarky, as each state still relies on foreign hardware. Duplication does fragment the pooled demand, which raises scale. Managed interdependence points to shared builds at the EU level.

Policy Recommendations

Two follow from the framework. The first is the capacity layer. The second is connecting the authority layer to this capability.

The EU should co-finance shared, permanent public sector capacity instead of national builds of projects in parallel (European Commission, 2021). The capacity of Europe to support open source institutions is far too small compared to the value open source gives. Co-financing based on cross-border reuse of platforms such as openDesk fills this gap and eliminates the redundancy Edler et al. (2023) find in the three platforms in the French, German, and Dutch. Pooled builds are of a scale that no single state can sustain, ensuring the continuity of the supply chain. A common codebase removes the need to go through a new development cycle for each buyer, which can take much longer to fix. Signalen shows the mechanism. Municipalities contribute a third of development costs and Amsterdam sponsors the rest. The platform has only 15 contributors compared to the 30 to 40 we estimate long-term sustainability needs (Linåker et al., 2026). EU co-financing would close this gap.

Second, member states should tie procurement to the sovereignty tiers and write exit terms into every sensitive contract. Specific workloads accept foreign-owned capacity. Sensitive tiers need EU control, but it is by effective control and not nominal ownership which is relevant for legal exposure. There are sovereign-by-construction platforms like Bleu, Delos, and S3NS to take over in the transition period, and the foreign technology under them does not provide any supply continuity. Exit terms set the duration to be fixed in advance if needed. The large contracts are split into lots for smaller European companies and parallel running is provided for in the transition. The Data Act's prohibition on switching charges from 12 January 2027 is the foundation (European Commission, n.d.). Transition comes at a cost. The Dutch Cloud Community, a trade association of domestic providers, estimates three to five years of parallel operation and faults the STACKIT agreement for giving domestic providers no chance to compete (Loohuis, 2026).

Neither recommendation works alone. Tiers without domestic supply reproduce the S3NS result, and a sensitive contract still runs on a US platform. Shared capacity without binding tiers allows buyers to default to the incumbent, as the Health Data Hub did. ECIPE puts the EU-US ICT and cloud investment gap at around $1.36 trillion and calls the sovereigntist framing misguided. For this reason, domestic champions would bring in capital and talent from other industries to fill a gap of this size, and open, free, and non-discriminatory access to global cloud capacity is cheaper (Bauer et al., 2024). The critique leaves the original exposure untouched. Cost doesn't change what the CLOUD Act requires an American firm to reveal, nor does it change what a foreign government will do to cut off. In doing so, researchers have not decided whether stronger contractual safeguards within an open architecture will reduce the exposure at lower cost. The tier-based design limits the question to sensitive workloads.

Conclusion

Setting the terms differs from controlling the infrastructure. A health database ran on Azure for six years after regulators found the arrangement unlawful. German public bodies kept using software their own regulators questioned, because no domestic alternative stood ready. Over the same period, the EU-based cloud share fell from roughly 29 to 15 per cent while the rulebook grew. Vendors changed their conduct under regulatory pressure, as the Brussels Effect predicts, yet buyers gained no option to leave.

The framework explains the pattern. Regulatory sovereignty sits in the authority layer and has advanced. Operational autonomy sits in the capacity layer and has stalled. Measured by legal exposure, supply continuity, and time to remedy, the main cases fail on at least one count.

Where the gap narrowed, member states did the work. France, the Netherlands, and Schleswig-Holstein acquired and operated capacity instead of certifying or fining. The EU role is narrower and still decisive: fund shared builds, set the control rule by tier, and force deadlines after findings.

The Tech Sovereignty Package is the most serious EU-scale response so far. Its flagship procurement nonetheless produced a winning bid running partly on Google Cloud. Rules exclude firms from a tier but do not create firms to fill the tier. Closing the gap demands supply, demand, and institutional capacity together, and member states have led that work with partial results. The next procurement round will test whether the EU builds capacity or writes more rules.

References

Bauer, M., Erixon, F., & Pandya, D. (2024, May 28). *The EU's trillion dollar gap in ICT and cloud computing capacities: The case for a new approach to cloud policy*. European Centre for International Political Economy. https://ecipe.org/publications/eu-gap-ict-and-cloud-computing/

Bertelsmann. (2024). *First sovereign cloud platform for the German administration on the home straight*. https://ber-cws-prod-web-release.azurewebsites.net/en/media/news/first-sovereign-cloud-platform-for-the-german-administration-on-the-home-straight.html

Bleu. (2026, May 15). *Collaborer et innover en confiance*. https://www.bleucloud.fr/

Bradford, A. (2019). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Congressional Research Service. (2025). *Cross-border data sharing under the CLOUD Act* (CRS Report No. R45173). https://www.congress.gov/crs-product/R45173

Davies, P. (2026, January 27). *France to ditch US platforms Microsoft Teams, Zoom for 'sovereign platform' citing security concerns*. Euronews. https://www.euronews.com/2026/01/27/france-to-ditch-us-platforms-microsoft-teams-zoom-for-sovereign-platform-amid-security-con

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. (2025, November 14). *HBDI: Microsoft 365 kann datenschutzkonform genutzt werden*. https://datenschutz.hessen.de/presse/hbdi-microsoft-365-kann-datenschutzkonform-genutzt-werden

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy, 52*(6), Article 104765. https://doi.org/10.1016/j.respol.2023.104765

European Commission. (n.d.). *Data Act explained*. Shaping Europe's Digital Future. Retrieved October 4, 2026, from https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

European Commission. (2021, September 21). *Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and

European Commission. (2026a, April 17). *European Commission awards €180 million tender for sovereign cloud to four European providers* [Press release]. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_833/IP_26_833_EN.pdf

European Commission. (2026b). *Proposal for a regulation on cloud and AI development* (COM(2026) 502 final). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0502

European Data Protection Supervisor. (2024). *European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies* [Press release]. https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security, 31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Garo, A. (2026, April 13). *La DINUM lâche Windows pour Linux et impose un plan de souveraineté à chaque ministère avant l'automne*. IT Social. https://itsocial.fr/logiciel-agilite/logiciel-agilite-actualites/la-dinum-lache-windows-pour-linux-et-impose-un-plan-de-souverainete-numerique-a-chaque-ministere-avant-lautomne/

Gundermann, C. (2026, August 7). *Brussels vs. Brussels: The EU's Data Act and the DMA's clash over cloud*. Center for Strategic and International Studies. https://www.csis.org/analysis/brussels-vs-brussels-eus-data-act-and-dmas-clash-over-cloud

Haeck, P. (2026, May 26). *Netherlands blocks US takeover of vital digital supplier*. Politico. https://www.politico.eu/article/netherlands-blocks-us-takeover-vital-digital-supplier/

Hale, C. (2026, March 19). *Dozens of European cloud CEOs call for real tech sovereignty ahead of Cloud and AI Development Act*. TechRadar. https://www.techradar.com/pro/dozens-of-european-cloud-ceos-call-for-real-tech-sovereignty-ahead-of-cloud-and-ai-development-act

Interoperable Europe Portal. (2025). *Open source for municipal services: Case study on Signalen*. https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/open-source-municipal-services-case-study-signalen

Khafo, S. (2025). *Procedure file 2025/2007(INI)*. Legislative Observatory, European Parliament. https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025/2007(INI)

Krempl, S. (2025, December 7). *Goodbye, Microsoft: Schleswig-Holstein relies on open source and saves millions*. Heise Online. https://www.heise.de/en/news/Goodbye-Microsoft-Schleswig-Holstein-relies-on-Open-Source-and-saves-millions-11105459.html

Linåker, J., Nummelin-Carlberg, A., & O'Riordan, C. (2026). Public sector open source program offices — Archetypes for how to grow (common) institutional capabilities. *Journal of Systems and Software, 241*, Article 112998. https://doi.org/10.1016/j.jss.2026.112998

Lomas, N. (2022, November 28). *Microsoft 365 faces darkening GDPR compliance clouds after German report*. TechCrunch. https://techcrunch.com/2022/11/28/microsoft-365-faces-darkening-gdpr-compliance-clouds-after-german-report/

Loohuis, K. (2026, September 24). *Netherlands designs sovereign cloud but concedes hardware dependency*. Computer Weekly. https://www.computerweekly.com/news/366651113/Netherlands-designs-sovereign-cloud-but-concedes-hardware-dependency

Marchandon, L. (2026, April 23). *France swaps Microsoft for Iliad's Scaleway to repatriate health data hub*. Reuters. https://www.reuters.com/world/europe/france-swaps-microsoft-iliads-scaleway-repatriate-health-data-hub-2026-04-23/

Martens, B. (2026, July 8). *How can Europe address its pressing AI compute infrastructure shortfall?* Bruegel. https://www.bruegel.org/policy-brief/how-can-europe-address-its-pressing-ai-compute-infrastructure-shortfall

McDermott Will & Emery. (2020, October 15). *Transfers of health data from France to the United States not prohibited... but must be protected by strong safeguards*. https://www.mcdermottlaw.com/insights/transfers-of-health-data-from-france-to-the-us-are-not-prohibited-by-the-french-data-protection-authority-or-french-courts/

Nicol-Schwarz, K. (2026, June 3). *Europe unveils tech sovereignty package amid growing concerns over reliance on U.S. tech: "We want to be sure nobody has a kill switch."* CNBC. https://www.cnbc.com/2026/06/03/europe-tech-sovereignty-us-tech-reliance.html

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4). https://policyreview.info/concepts/digital-sovereignty

Sénat. (2025, June 9). *CE commande publique : Compte rendu de la semaine du 9 juin 2025*. https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html

Stojčić, N., Srhoj, S., & Coad, A. (2020). Innovation procurement as capability-building: Evaluating innovation policies in eight Central and Eastern European countries. *European Economic Review, 121*, Article 103330. https://doi.org/10.1016/j.euroecorev.2019.103330

Uyarra, E., Zabala-Iturriagagoitia, J. M., Flanagan, K., & Magro, E. (2020). Public procurement, innovation and industrial policy: Rationales, roles, capabilities and implementation. *Research Policy, 49*(1), Article 103844. https://doi.org/10.1016/j.respol.2019.103844

EPIS