

Avoiding the Kill Switch: Europe's Digital Sovereignty Dilemma

Charles Pahud de Mortanges*

It's so obvious that it's not a good idea to be a digital colony of the US.

And I think we have a window right now to break out of that.

— MEP Alexandra Geese (Greens/EFA, Germany), January 2026

The Kill Switch, Activated

In early 2025, the Trump administration issued executive orders sanctioning officials of the International Criminal Court, following the ICC's arrest warrants for two Israeli political leaders. In the months that followed, something remarkable occurred on European soil: judges and prosecutors of an international legal institution found their Microsoft accounts suspended, their email access denied, and their connections to financial platforms severed. Not because of a cyberattack. Not because of a technical failure. Because those platforms operate under American jurisdiction and must comply with American sanctions law.¹

The phrase that began circulating in European policy circles was “kill switch.” The idea was simple and alarming. Cloud services, payment systems, communication platforms, entire categories of data infrastructure: all of it could be rendered inaccessible not by technical failure but by a political decision taken in a foreign capital, transmitted through the private companies that control the servers and algorithms on which European institutional life increasingly runs.

The ICC episode, striking as it was, targeted named individuals and specific institutions. What followed in June 2026 was something blunter. The Trump administration invoked export control authority to bar all foreign nationals from Anthropic's most advanced AI models, Fable 5 and Mythos 5. Since nationality cannot be verified at the user level, Anthropic had no choice: it disabled both models for every customer on earth, American and non-American alike. The company stated publicly that it had received only “verbal evidence of a potential narrow, non-universal jailbreak.”² It disagreed with the assessment. The models went dark anyway. The

* Charles Pahud de Mortanges is (Full) Professor Emeritus at the University of Liège (Belgium).
c.pahud@uliege.be

¹The ICC episode is documented in detail in the Soufan Center IntelBrief of February 26, 2026, and in reporting by TechCrunch, April 10, 2026.

²Anthropic, "Fable and Mythos Access Update," blog post, June 13, 2026 (<https://www.anthropic.com/news/fable-mythos-access>). Reported by Al Jazeera, June 14, 2026; PBS NewsHour, June 13, 2026; Time, June 13, 2026.

Pentagon's chief information officer offered her commentary on social media: "America First. Always."³

Three days before the Fable/Mythos order, European Commission President Von der Leyen had used the same phrase at the launch of the EU's Tech Sovereignty Package. "We want to be sure nobody has a kill switch."⁴ It was no longer think-tank jargon. It had become policy language.

The question here is not whether European digital dependency is real. That case has been made. The question is how Europe arrived at this position, what it is doing about it, and whether any of it is working fast enough.

The Anatomy of a Digital Colony

Start with the numbers. Three American companies (Amazon Web Services, Microsoft Azure, and Google Cloud) supply approximately 70% of Europe's cloud computing infrastructure.⁵ More than 80% of European AI chatbot users rely on OpenAI's ChatGPT. Europe holds only 5% of global computing infrastructure and attracts roughly 6% of global venture capital in artificial intelligence.⁶ Between 2013 and 2024, American private investment in AI totaled \$109.1bn. Europe managed \$19.42bn over the same period.⁷

These are not the statistics of a partnership. They are the reality of structural dependency: what MEP Axel Voss calls being a "digital colony" of the United States, and what Mistral CEO Arthur Mensch described at Davos as a situation where "95% of digital services and AI are imported from the US."

There is a distinction worth making, and the EU has spent a decade blurring it. Economic dependency and political vulnerability are not the same thing. A European firm paying advertising rents to Google is transferring economic surplus to a foreign provider. A European institution whose email is suspended because of a decision at the US Treasury is losing its capacity to function. A European researcher whose access to an advanced AI model is revoked by executive order is losing a working tool, irrespective of her contractual relationship with the provider. The first is a market problem. The second and third are sovereignty problems. They require different instruments.

The dependency extends beyond software platforms. Elon Musk's Starlink provides satellite internet coverage across much of Europe, including, most pointedly, Ukraine, where it has been operationally essential for military communication. When the United States reportedly threatened to suspend Starlink access unless Ukraine signed a minerals deal, the vulnerability for any critical infrastructure controlled by a foreign

³Kirsten Davies, post on X, June 13, 2026, cited in Al Jazeera, June 14, 2026.

⁴European Commission press conference, June 3, 2026. See also: "Europe unveils tech sovereignty package amid growing concerns over reliance on U.S. tech," CNBC, June 3, 2026.

⁵Krištopaitytė, E. (January 7, 2026). "Europe has powerful weapons against Trump and his tech bros. Will it use them?" Cybernews.

⁶Schaefer, P. (January 26, 2026). "How the EU became a digital colony – and how it might break free." The Parliament Magazine. Figures from a December 2025 report by RAND and the Centre for Future Generations.

⁷Krištopaitytė, E. (January 7, 2026). Cybernews.

actor subject to political influence became concrete.⁸ Ukraine was the preview. Europe is watching.

How Europe Fell Behind

The dependency did not emerge from a deficit of scientific quality. European research in statistics, pattern recognition, and machine learning was on par with the United States well into the 2000s.⁹ The divergence came in the 2010s, when AI progress shifted from algorithmic advances to compute-heavy model training, a shift that requires massive, long-horizon capital investment and tolerance for extended financial loss.

American investors were loss tolerant. European investors were not. While the technology boom in the United States generated the self-reinforcing feedback loop of capital, infrastructure, prestige, and talent that produced OpenAI and Google DeepMind, European firms were optimising for profitability, and European regulators were writing framework documents. Economists have a name for this pattern: the Matthew Effect.¹⁰ Advantages compound. Those with initial leads accumulate more. Those behind fall further back.

Platform fragmentation compounded the problem. Unlike the United States, which constitutes a single unified digital market of 335 million people sharing one language and one legal system, the European Union comprises 27 member states with different languages, legal traditions, and regulatory environments. A startup scaling across the EU confronts 24 official languages and 27 national implementations of EU directives. An American technology company, already at scale from its domestic market, can enter Europe as a finished product. A European startup must build for Europe from scratch.

The result: Europe produced no competitive search engine, no significant public cloud provider, no social network at scale, and no mobile operating system. The closest thing to a European AI champion is Mistral, a Paris-based firm valued at \$13.7bn. Admirable, by European standards. OpenAI is valued at \$500bn. Mistral commands roughly 2% of the European AI chatbot market.¹¹

The Geopolitical Accelerant

The structural dependency predates the Trump administration's return to office. What the second Trump term changed was the political salience of that dependency, and the speed with which European governments concluded it constituted a strategic liability rather than merely an economic one.

Vice President Vance's speech at the Munich Security Conference in early 2025, Trump's repeated claims to Greenland's territory, and an approach to allied relations

⁸Ibid.

⁹Harry Law, quoted in Schaefer, P. (January 26, 2026). The Parliament Magazine.

¹⁰Merton, R.K. (1968). "The Matthew Effect in Science." *Science*, 159(3810), 56–63.

¹¹Schaefer, P. (January 26, 2026). The Parliament Magazine.

that treats decades-old commitments as negotiable: together they prompted a reassessment that would have seemed alarmist two years earlier. If the United States is willing to use economic and technological leverage against allies as well as adversaries, the ICC episode is not an anomaly. It is a prototype. Europe is the test case.

The escalation since January 2025 has followed a recognisable pattern. The Trump administration imposed a visa ban on Thierry Breton, former EU commissioner and architect of the Digital Services Act, citing European “coercion of American platforms.” The US Trade Representative warned of retaliatory consequences for European service providers if EU “discrimination” against American companies continued. Trump linked tariff reductions explicitly to the softening of European digital regulation.¹²

The Fable/Mythos episode crossed a categorical threshold. Until June 2026, the United States had used export controls primarily against hardware: chips, lithography machines, the physical infrastructure of AI. Those restrictions were one step removed from the end user. Restricting the models themselves is a different order of intervention. It reaches directly into the service layer where most European institutional and commercial activity operates. The United States has now claimed sovereign authority over who may access its most powerful AI systems, regardless of where those users live or what they are doing.

There is a further dimension. On 9 March 2026, Anthropic sued the Trump administration over a separate dispute involving military AI applications. The export control order arrived in the middle of that litigation. This is worth reflecting on. European users of American AI systems are exposed not only to the US legal framework, but to whatever is happening politically between their software provider and Washington on any given week. That is a new kind of risk.

A further episode, on 25 June 2026, introduced a related but distinct form of control. On that day, the White House instructed OpenAI to restrict its forthcoming GPT 5.6 model to a small group of government-approved “trusted partners.” Where Fable/Mythos illustrated retroactive denial, GPT 5.6 illustrates prospective gatekeeping: Washington asserting the authority to determine, before a model reaches the market, who will be permitted to use it. European users and institutions are not on that list, and were not consulted in its construction.¹³

The Commission’s instinct for accommodation has not served it well. In late 2025, it proposed a “Digital Omnibus” package simplifying data and AI rules. Washington rejected it as insufficient. EU lawmakers were more resistant. In April 2026, European Parliament members fell out with the Commission over plans to open a dialogue with Washington about EU tech regulation. The fear: that it would water down the bloc’s digital laws to obtain goodwill that Washington had no intention of granting. Alexandra Geese described allowing US officials into those talks as letting platforms “grade their own homework.”¹⁴ She had a point.

¹²Krištopaitytė, E. (January 7, 2026). Cybernews.

¹³Capoot, A. (June 26, 2026). "OpenAI limits new AI models to 'trusted partners' at request of U.S. government." *CNBC*.

¹⁴GlobalData / Yahoo Finance, April 13, 2026.

What Europe Is Actually Doing

Regulation and Its Limits

The EU's primary response to platform dominance has been regulatory. The GDPR, the Digital Markets Act and Digital Services Act, the AI Act, the Data Act: taken together, they constitute arguably the world's most ambitious regulatory framework for digital platforms. They have also, through what scholars call the "Brussels Effect," reached beyond European borders.¹⁵ Firms that want access to the single market cannot afford to maintain separate compliance regimes, so EU standards tend to become de facto global ones.

The problem is that regulating behaviour and reducing dependency are not the same thing. A European institution relying on Microsoft Azure is no less dependent on Microsoft after GDPR than before it. The regulation changes what Microsoft can do with the data. It does not change whether the institution can function without Microsoft. Cristina Cafarra, founder of the EuroStack Industry Initiative, put it without ceremony: "It has become the sole obsession of Europe for months to tame Big Tech. News flash. We were not taming, we are not taming, and we will not tame Big Tech."¹⁶

There is a further problem that no existing regulation can address. The DMA and GDPR assume American platform providers are commercially motivated actors: they want access to the European market, so they will comply with European rules. The ICC episode showed this assumption has limits. Under certain political conditions, those firms can be instructed by their home government to override the commercial calculation entirely. The Fable/Mythos episode revealed something beyond that. A US export control order can sever access to a commercial AI product through a direct government instruction, based on a disputed security finding, with only verbal notice to the company. No compliance officer in Brussels addresses this scenario. No regulation yet written covers it.

Government Migration: The Concrete Steps

The most visible recent development has been government-level migration away from American platforms, driven not by regulatory framework but by political shock. France has moved furthest and most publicly. In April 2026, the French government announced plans to migrate computers at DINUM, its central digital agency, from Microsoft Windows to Linux. French minister David Amiel put the objective plainly: the government "can no longer accept that it does not have control over its data and digital infrastructure."¹⁷ France had already dropped Microsoft Teams in favour of Visio, a French-made tool, and announced plans to migrate its health data platform to a trusted European system by year's end. Austria has moved its defence ministry to open-source software. Belgium and Germany have expanded domestic alternatives for public administration. The pattern is consistent: it is governments that have acted, not markets.

¹⁵Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

¹⁶Cafarra, C., quoted in Schaefer, P. (January 26, 2026). *The Parliament Magazine*.

¹⁷TechCrunch, April 10, 2026.

The longer-run case of the German state of Schleswig-Holstein is instructive. Having first considered moving away from Microsoft in 2011, its cabinet formally agreed in 2024 to replace all Microsoft products with open-source alternatives. Progress has been genuine but not frictionless: managing security across multiple open-source providers requires considerably more internal expertise than relying on Microsoft's consolidated security architecture.¹⁸ The lesson is not that open-source migration is impossible. It is that it is slower and more demanding than its advocates initially project.

Industrial Policy: The June 2026 Package

The most ambitious response goes beyond regulation and procurement. It proposes rebuilding Europe's digital supply chain from its foundations. The label attached to this vision is "EuroStack," and on June 3, 2026, the European Commission gave it its most concrete legislative form yet. The Tech Sovereignty Package comprises two legislative proposals, the Cloud and AI Development Act (CADA) and the Chips Act 2.0, alongside a new Open Source Strategy and a roadmap for AI in energy.¹⁹ The numbers are large: €200bn for data centres by 2036, €100bn for cloud and AI, €2bn for open-source software over seven years. The stated goal is to triple EU data centre capacity by 2035.

The CADA's most significant element is its EU Cloud Sovereignty Framework. It establishes four assurance tiers for cloud and AI services used by public authorities. At the highest two tiers, US hyperscalers are effectively disqualified from the most sensitive government contracts. The reason is structural. The US CLOUD Act permits American law enforcement to request user data from American companies regardless of where that data is stored. This jurisdictional reach prevents American providers from meeting the legal independence criteria of the top tiers.²⁰ Executive Vice-President Henna Virkkunen acknowledged this directly: it would be "difficult" for US companies to reach the highest sovereignty levels. The US law that governs them makes it so.

This is a genuine advance over the pure GDPR logic. For the first time, the EU is proposing to address not just what providers can do with data, but whether their structural exposure to American law disqualifies them from certain categories of European public-sector work. The caveat is that the proposal must survive legislative enactment, implementation will take years, and "sensitive government contracts" covers a far smaller perimeter than European institutional and commercial life as a whole.

It is also worth noting what the package does not yet address. The Fable/Mythos export control order was not a CLOUD Act request. It was a distinct legal instrument targeting access to a commercial AI model by nationality. The EU's sovereignty framework addresses jurisdictional reach over data at rest. It has no current response to the scenario in which the US government restricts access to a commercial AI service

¹⁸GlobalData / Yahoo Finance, April 13, 2026.

¹⁹European Commission, IP/26/1187, June 3, 2026.

²⁰"The EU Cloud and AI Development Act in Depth," Inside Global Tech, June 11, 2026. See also: "EU Unveils Sweeping Tech Sovereignty Push," TechPolicy.Press, June 2026.

through a direct export control order. That is a different layer of the technology stack. The EU's legislative cycle has not caught up with it.

Europe's Leverage

The dependency runs in one direction. But not entirely. ASML, the Dutch company, holds a virtual global monopoly on extreme ultraviolet lithography machines: the equipment without which the most advanced semiconductors, including the Nvidia chips powering American AI, cannot be manufactured. Julia Hess of the Interface think tank calls it a “perfect choke point.”²¹ The complication is that using it would require unanimous agreement across 27 member states, and the semiconductor supply chain's interdependence means any restriction carries significant collateral costs. Europe holds the choke point. It has been reluctant to squeeze.

The Anti-Coercion Instrument, introduced in 2023, allows the EU to respond to economic coercion with tariff increases and exclusion from public procurement. Von der Leyen has suggested applying it to the advertising revenues of US digital platforms.²² Whether she means it remains to be seen.

The Brussels Effect remains perhaps the most durable lever of all, provided the EU resists the diplomatic temptation to accommodate itself into irrelevance. Lena-Maria Böswald at Interface has noted an uncomfortable paradox: the more frequently the EU describes itself as not being a censorship regime, the more the word “censorship” adheres to it.²³ The defensive posture is the least effective one available.

Does Any of This Work?

The honest answer is: partially, and not yet for the most consequential problem.

Regulation has genuine effects, but a decade of it has not reduced Europe's structural dependency on American platforms. The CADA's sovereignty framework is the most direct policy response yet to the jurisdictional problem the ICC episode revealed. But it must pass the Parliament and Council. It will take years to implement. And it does not touch the model-layer scenario the Fable/Mythos episode introduced.

Where movement has been fastest is at the government level (France, Austria, Schleswig-Holstein), driven by political shock rather than regulatory framework. There is an uncomfortable truth embedded here: the Trump administration's conduct has accelerated European digital sovereignty initiatives more effectively than a decade of Commission policy documents.

Nicole Lemke's observation at Interface provides a more tractable benchmark: European AI models do not need to reach the global frontier to displace American competitors in European markets. They need to be good enough, compliant with European data protection standards, and trusted by European users and institutions.²⁴ That is a narrower and more achievable target. Zach Meyers of the Center on

²¹Hess, J., quoted in Krištopaitytė, E. (January 7, 2026). Cybernews.

²²Von der Leyen, U., quoted in Krištopaitytė, E. (January 7, 2026). Cybernews.

²³Böswald, L.-M., quoted in Krištopaitytė, E. (January 7, 2026). Cybernews.

²⁴Lemke, N., quoted in Schaefer, P. (January 26, 2026). The Parliament Magazine.

Regulation in Europe points to SAP's dominance in American enterprise software as evidence that deep integration can produce mutual dependency with its own deterrent logic.²⁵ The argument has merit, but it assumes a reciprocal dependency that Europe does not currently possess in the infrastructure layer.

Cafarra's point stands: a "Buy European" provision in public procurement requires no new technology and no new legislation.²⁶ That EU institutions run on Microsoft Teams is not a market outcome. It is a procurement decision. And procurement decisions can be changed.

A Realistic Assessment

Three time horizons suggest themselves. In the short term: triage. Not all cloud computing carries the same political risk. Government communications, legal institutions, health data, defence-related systems: these are the areas that a US sanctions order or export control directive can reach. Commercial transactions are a different matter. Prioritise the sensitive ones. Migrate them first to European-controlled infrastructure outside American jurisdictional reach.

In the medium term: procure differently. A serious "Buy European" requirement in public procurement would simultaneously create revenue for European software firms and reduce institutional dependency. The willingness to act on stated priorities, rather than merely to articulate them, is the distinguishing variable.

In the longer term: build. The EuroStack vision requires capital, consolidated cloud infrastructure, competitive AI models, and a procurement culture that backs European technology firms before they reach scale rather than after. This is the most consequential time horizon of the three. Governments and institutions that build AI dependency on American foundation models now will face the same structural lock-in in 2030 that cloud dependency has produced today, only more deeply embedded in their workflows. The window to choose differently is shorter than it appears.

Lasting Rupture or Temporary Fracture?

A February 2026 Soufan Center analysis framed the question precisely: does current European technological decoupling represent a "lasting fissure or temporary fracture" in the transatlantic relationship?²⁷

On present evidence, the decoupling is real but gradual. The June 2026 Tech Sovereignty Package tilts the evidence marginally toward rupture: legislative proposals requiring member states to conduct sovereignty risk assessments and bar US hyperscalers from sensitive contracts represent structural choices, not political gestures. But the pace remains slower than the urgency demands. And the urgency itself keeps escalating.

The ICC episode illustrated the kill switch as a targeted instrument: specific institutions, specific individuals, specific sanctions orders. The Fable/Mythos order

²⁵Meyers, Z., quoted in Schaefer, P. (January 26, 2026). The Parliament Magazine.

²⁶Cafarra, C., quoted in Schaefer, P. (January 26, 2026). The Parliament Magazine.

²⁷Soufan Center IntelBrief, February 26, 2026.

illustrated something blunter. Hundreds of millions of users. No adequate notice. A disputed security finding. A social media post from a Pentagon official as the accompanying explanation. European users of American AI systems are not merely exposed to the US legal framework. They are exposed to the political temperature of the relationship between their software provider and Washington, which on any given week may include active litigation between the two.

No serious European analyst argues for a complete break. The argument is more targeted. Sufficient independent infrastructure, so that the ICC episode cannot repeat itself against European institutions. Sufficient European AI capacity, so that a new layer of dependency does not form in the model layer on top of the cloud layer already present. Sufficient regulatory credibility, so that existing rules can be enforced without diplomatic capitulation to the country whose companies those rules most directly affect.

What the current political moment has provided is urgency, and urgency is not nothing. The question is whether it converts into industrial capacity before the next executive order arrives. Nobody knows when that will be. The window is open. It will not remain so indefinitely.