

POLICY BRIEF

Defending Europe's Digital Sovereignty

Insulating enforcement, simplifying the rulebook and building a European technological base

College of Europe · Institute for European Studies (IEE-ULB) | Authors: Luca Brocato · Filippo Roncato

Brussels · 4 June 2026

KEY MESSAGES

Europe's digital rulebook cannot deliver sovereignty by itself. The DMA, DSA and AI Act fall mainly on dominant US firms, so Washington treats them as disguised taxes and ties their enforcement to trade, gaining leverage over a politicised Commission.

RECOMMENDATION 1

Delegate enforcement of the Digital Services Act to an independent EU agency modelled on AMLA, allowing it to be shielded from political pressure and undermining Washington's bargaining lever.

RECOMMENDATION 2

Simplify the digital rulebook to support European competitiveness through regulatory ambition.

RECOMMENDATION 3

Back regulatory sovereignty with industrial capacity by building the EuroStack, a sovereign, open and federated European technological base resting on guaranteed public procurement, pooled investment and open standards.

Introduction

Digital sovereignty has moved to the centre of the debate on European strategic autonomy. The cloud services, online platforms and artificial-intelligence and large-language models on which European economies, administrations and citizens increasingly rely are supplied overwhelmingly by a small number of firms based in the United States. This dependence is a serious strategic weakness: even where the operational risk of relying on US providers is low, Washington can gain leverage across policy domains, from tariffs to defence. Digital sovereignty is therefore a question of both competition policy and, most importantly, strategic autonomy.

Europe's response has so far been largely regulatory: the Digital Markets Act (DMA), the Digital Services Act (DSA) and the Artificial Intelligence Act (AI Act) together form the world's

most ambitious digital rulebook. Rules alone, however, cannot secure sovereignty. Because their main addressees are American firms holding near-monopoly positions in their markets, these regulations are increasingly read in Washington as a *de facto* tax on US companies, and their enforcement has become entangled with wider questions of trade and security. A Commission that now acts as a political player as much as a technical one can be pressed to trade lighter enforcement for concessions elsewhere, and that is indeed what has happened: in spring 2025 it threatened a levy on US digital services in response to American tariffs, yet only a year earlier it had stripped from its draft cloud-certification scheme the sovereignty requirements that would have curbed the dominant American providers. As Vice-President Teresa Ribera has warned, the United States exploits this malleability to 'blackmail' the Union in policy negotiations.

This brief argues that defending Europe's digital sovereignty means acting on two fronts: European regulation and European products. It advances three recommendations to that end. The first entrusts enforcement of the rulebook to an independent agency, beginning with the DSA, to shield it from political leverage. The second simplifies the rulebook itself, aiming to reinforce

competitiveness instead of undermining it. The third moves from regulation to industrial capacity: Europe must build a sovereign technological base, the EuroStack, as regulatory sovereignty alone is not enough. The sum of these recommendations highlights sovereignty not as a synonym for protectionism, but as a condition to set and enforce its own rules.

RECOMMENDATION 1

Delegate DSA enforcement to an independent EU agency

The first recommendation concerns the body that enforces the rules: enforcement should be delegated to an independent agency rather than concentrated in the Commission. This case is not uniform across the rulebook: structural separation currently suits neither the DMA nor the AI Act, but for the DSA it is both desirable and feasible.

Several considerations support independence. Taking enforcement out of the Commission's hands strengthens credibility and technical expertise, while protecting decisions from electoral swings and political convenience. The empirical evidence confirms this: formal independence measurably improves the quality of competition enforcement, while politically dependent regulators are far less likely to act against firms, partly because they are more exposed to lobbying. As Mariniello argues, independence matters most when enforcement comes under external pressure linked to trade, as happened during the EU-US trade negotiations of 2025. So long as the Commission can yield, the American threat of retaliation stays credible and Brussels has an incentive to soften enforcement in advance. Once enforcement is placed beyond the Commission's reach, the Union can no longer offer to hold back from applying its own rules and the equilibrium moves towards enforcement without retaliation, neutralising the threat. An independent agency works, in short, as a safeguard against leverage, removing the bargaining asymmetry described above.

Independent EU agencies with direct supervisory

and sanctioning powers already exist. The Meroni doctrine has been progressively eroded: the 2014 ESMA short-selling judgment allows delegated powers to carry a bounded margin of discretion, provided they rest on objective criteria and remain subject to judicial review. The establishment of AMLA in 2024 confirms that a substantial transfer of enforcement authority is compatible with EU law. Both ESMA and AMLA can investigate, bind and fine private entities, and answer only to the Court of Justice.

The recommendation is aimed at the DSA rather than the DMA or the AI Act due to the Acts' natures. The DMA is bound up almost entirely with competition policy; separating it would sacrifice synergies between Commission services and risk duplicated proceedings. The AI Act governs a framework still in flux, currently being amended through the Digital Omnibus before it enters full force, and stripping enforcement expertise out of the Commission at this stage would put future legislation at risk. The DSA, through its link to freedom of expression, is the regulation most exposed to political pressure, internal and external alike: a US congressional report has described it as an instrument of global censorship and the Polish president vetoed the national implementing law in 2026. The risk of distortion is higher and the gain from independence larger, while the costs are limited, since the DSA's obligations are stable and its discretion is already framed by Commission guidelines, codes of conduct and delegated acts.

We therefore propose a dedicated DSA agency modelled on AMLA. The Commission would keep the power to designate the platforms in scope, while the agency would take over supervision, investigation, infringement decisions and

sanctions, applying the law independently. The supervisory fee the DSA already levies could give it budgetary autonomy, with the Court of Justice exercising final review.

RECOMMENDATION 2

Simplifying the digital rulebook

The Union built its digital rulebook at remarkable speed, layering the GDPR, DMA, DSA, AI Act, Data Act and NIS2 on top of one another within a decade, creating a cumulative problem. A 2025 European Parliament study of their interplay finds that obligations which are reasonable in isolation combine into duplicative, inconsistent or unclear requirements, deterring uptake and slowing new products' access to the market. For instance, the AI Act's fundamental-rights impact assessment and the GDPR's data-protection impact assessment apply to the same systems but differ in scope, supervisor and procedure, so a single deployment triggers two parallel exercises before two different authorities. The AI Act and the Cyber Resilience Act, reinforced by NIS2, impose overlapping cybersecurity and incident-reporting duties on the same products. This ambiguity favours the best-resourced players, who are ready to absorb the costs, and weighs on smaller entrants which were supposed to benefit from the rulebook.

The Commission has responded with its "Omnibus" simplification packages, most recently the Digital Omnibus of November 2025. As Mariniello shows, the proposals have moved forward without the impact assessments normally required, so their distributive effects remain undisclosed and the Commission cannot be held to account for the trade-offs it asks legislators to accept. The exercise is also driven by a single objective, closing the gap with the United States, and that objective is analytically weak. European and American markets

perform differently because they protect rights differently; comparing the two to end up blaming the difference in European rules is ineffective. The common complaint that the GDPR raises costs does not take into account that the cost is that of protection, not of inefficiency.

Simplification should therefore be surgical. In the short term, regulators can act without new legislation by issuing joint guidance and recognising one another's impact assessments, so that a single exercise satisfies overlapping obligations. In the medium term, targeted legislative fixes should close the definitional gaps that generate most of the uncertainty, above all the question of what counts as a high-risk AI system, and harmonise the cybersecurity and reporting duties that the AI Act, the CRA and NIS2 currently impose in parallel. In the long term, the Commission should acknowledge its aim of narrowing the transatlantic gap and clearly take responsibility for the distributive choices.

The principle is that of simplification instead of deregulation, aiming for a cleaner and more coherent rulebook, not an empty one. "Streamlining" must not become a cover for political concessions to external pressure, in line with Recommendation 1. Simplification should make the DSA and its companion instruments easier to follow and harder to ignore, with a rulebook that would finally reinforce Europe's sovereignty.

Building a European alternative for technological sovereignty

The first two recommendations concern how Europe regulates digital markets; this one concerns what Europe's alternatives are. Rules cannot deliver sovereignty when the infrastructure they govern is almost entirely foreign. More than 80% of Europe's digital technologies and infrastructure are imported. Around 70% of the foundational AI models in use were developed in the United States; three American 'hyperscalers' control over 65% of the European cloud market, while the largest European provider holds barely 2%; and the EU manufactures under 10% of the world's semiconductors. Only four of the world's top 50 technology firms are European, and Draghi estimates that digitalising and decarbonising the economy will require raising investment by some five percentage points of GDP. As the preceding sections argued, this dependence also hands external powers structural leverage: when the firms supplying Europe's cloud, chips and models are the same firms its regulators must discipline, enforcement becomes an object of trade negotiations. For this reason, regulatory sovereignty needs to stand on industrial capacity.

Closing this gap is the purpose of the EuroStack initiative, which treats Europe's digital base as a single layered stack, from raw materials and energy through chips, networks, devices, cloud and software up to data and AI. EuroStack does not argue for autarky, which its authors consider 'neither feasible nor desirable'. The aim is open, interoperable and federated European capacity in strategic layers, not simple import substitution. The report proposes mobilising €300 billion over ten years, anchored by a European Sovereign Tech Fund with an initial €10 billion to build and scale

demonstrator services selected through open competition.

First, demand has to be guaranteed through procurement. The Cloud and AI Development Act proposed by the Commission in June 2026 would establish an EU-wide cloud-sovereignty framework and require public bodies to assess their needs and source sovereign cloud services; extending such 'buy European' criteria across public IT would give domestic providers the stable demand that grants alone cannot supply. Second, investment must be pooled together: scaling up the Sovereign Tech Fund (Germany's national equivalent received just €17 million in 2024) and federating compute through EuroHPC and the planned AI gigafactories would deliver the scale that Europe's firms need. Third, open-source software and mandated interoperability should become the default for public infrastructure, closing off the vendor lock-in that undermined earlier efforts.

The EuroStack report highlights warnings and dangerous precedents. Gaia-X, the previous flagship cloud project, stalled amid competing national agendas, bureaucracy and the absence of a common vision. Draghi cautions that displacing the hyperscalers outright is unrealistic, since the investment required would drain resources from fields where Europe can still lead, and the priority should instead be a foothold in more essential domains: sovereign cloud, chips, AI and digital identity. Energy is a further constraint, as surging data-centre demand meets a grid and a price structure not yet built for it. The lesson is to concentrate funding, guaranteed demand and open standards on the layers where dependence is most dangerous to defend strategic autonomy.

Conclusion

Europe's digital dependence is a structural condition that limits its freedom across trade, security and the rule of law. This brief has argued that the Union cannot regulate its way to sovereignty while the infrastructure it seeks to govern, and much of the political leverage over its own institutions, lies beyond its borders. This is why the three recommendations are to be read

together. Insulating enforcement from political pressure ensures credibility in the rules Europe has already written; simplifying the rulebook turns those rules into support for European industry; and building a sovereign technological base builds the foundation for autonomy. These recommendations would turn a defensive posture into strategic autonomy and remove the leverage that makes Europe's own rules negotiable.

REFERENCES

- Bria, F., Timmers, P. & Gernone, F. (2025). *EuroStack — A European Alternative for Digital Sovereignty*. Bertelsmann Stiftung, with CEPS, Stiftung Mercator and UCL IIPP.
- Court of Justice of the European Union (2014). *United Kingdom v Parliament and Council* (ESMA short-selling), Case C-270/12.
- Draghi, M. (2024). *The Future of European Competitiveness*. European Commission.
- European Commission (2026). Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (*Cloud and AI Development Act*), COM(2026) 502 final, 3 June 2026.
- European Commission (2026). *Strengthening Europe's tech sovereignty* (European Technological Sovereignty Package), 3 June 2026.
- European Parliament (2025). *Interplay between the AI Act and the EU digital legislative framework*. Study for the Committee on Industry, Research and Energy (ITRE), Graux, H., Garstka, K., Murali, N., Cave, J. & Botterman, M., PE 778575.
- Mariniello, M. (2025). *Efficiency and distribution in the European Union's digital deregulation push*. Bruegel Policy Brief, Issue 31/25, November 2025.
- Mariniello, M. (2026). *The case for a European Union digital enforcement authority*. Bruegel Policy Brief, Issue 05/26, March 2026.
- U.S. House Committee on the Judiciary (2025). *Foreign Censorship Threat: How the European Union's Digital Services Act Compels Companies to Censor Americans*.
- 'Captured by American clouds': the political economy of Gaia-X and European cloud sovereignty (2025). *Information, Communication & Society*.