Digital Sovereignty: How European Governments Undermine What They Claim to Build.

Bernard Sfez - 2026-02-20 08:15

Europe has the laws, the labels, and the rhetoric for digital sovereignty. What it lacks is consistency. Between legislation passed and contracts signed, a stubborn gap undermines the credibility of the whole project. From government procurement to school IT, tangible progress coexists with concessions that are hard to defend. Most troubling: it is in classrooms, year after year, that an addiction to closed ecosystems is being quietly built on the taxpayer's dime.

We examine what works, what doesn't, and why coherence remains the weakest link in an otherwise ambitious strategy. Sovereign alternatives exist and are proven. The only missing ingredient is the political will to scale them, from the classroom to the data-center.

Governments vs. Big Tech: Between Political Will and Structural Inertia

Real Political Signals

It would be unfair to say nothing is moving. Since the mid-2010s, European governments — led notably by France and Germany — have championed the idea of strategic digital autonomy, and recent years have seen a notable acceleration. However, information, intelligence, and cybersecurity specialists, as well as independent consultants working with public institutions, consistently highlight the slowness and sometimes the contradictions of public policy in this area : lack of follow-through, inconsistencies between rhetoric and action, and absence of consistency in execution.

In June 2025, during a dedicated Cabinet meeting, the French government officially acknowledged the severity of the situation: 83% of European digital spending is directed toward non-European actors, representing an estimated annual outflow of €264 billion according to the Asterès study commissioned by Cigref (April 2025). A figure that reflects not merely a market preference, but a structural dependency — which Cigref now compares to the EU's energy bill (€360 billion in 2024).

The political response has taken shape around several concrete axes:

The creation of a Digital Sovereignty Observatory

France officially launched its Digital Sovereignty Observatory on 26 January 2026, under the High Commission for Strategy and Planning. At EU level, the European Commission is pursuing a parallel initiative: a call for evidence on open digital ecosystems, published in January 2026, will feed into an EU-wide strategy expected in Q1 2026 — covering dependency mapping, open source, and sovereign cloud.

The "Cloud by Default" doctrine

Several European countries and the EU itself have adopted cloud-first policies for public administrations. France's "Cloud at the Centre" doctrine has been explained in detail by Cloud Temple (English), while the broader EU approach is set out in the European Commission's Cloud Computing Strategy. In summary, new IT projects in public administrations must use the cloud as the default hosting mode.

Trusted Cloud certification schemes

For sensitive data — national security, public health, critical personal data — hosting providers must meet rigorous security standards. France's SecNumCloud qualification (issued by ANSSI) and Germany's BSI C5 framework both guarantee not only a high level of cybersecurity (based on ISO 27001), but above all immunity to extraterritorial laws — meaning the provider cannot be compelled by a foreign government (typically the United States via the Cloud Act or FISA) to access your data. As explained by Clever Cloud, this is the key distinction between certified European cloud and US hyperscalers.

Investment plans for digital sovereignty

Horizon Europe and national recovery plans have mobilised significant funding for strategic technologies — cloud, AI, cybersecurity, quantum computing. The EU's Digital Decade investment targets and France's France 2030 plan aim to foster competitive European cloud IaaS/PaaS offerings, particularly for AI.

These initiatives are real and already represent a concrete acknowledgement of the problem. They deserve recognition. But they run into a structural issue we will now examine.

The Public Procurement Paradox

The detail of public cloud spending figures reveals a striking paradox. According to Eurostat (February 2026), 53% of EU enterprises now use paid cloud services — a 7-point increase in two years. Yet the direction of that spending tells a different story: as the Asterès/Cigref report confirms, 80–83% of European cloud and software spending flows to US providers. Public procurement of sovereign-certified solutions remains a marginal fraction of total cloud spending — while the rest flows largely to American hyperscalers.

In other words, governments are telling their administrations to choose sovereign options... while massively funding non-sovereign alternatives. As detailed in our previous article, these companies are subject to US law — the Cloud Act, FISA and the Patriot Act — and can be compelled to hand over user data, or cut off access to their services, on a simple order from a US court.

This paradox is glaring: the state exhorts its administrations to pursue sovereignty while injecting millions into the coffers of those who undermine it. Public procurement actively finances the

American digital giants, thereby inflicting a real stab in the back to European companies and actors who, without complaint, bear the additional costs of transforming toward digital independence.

The share of European actors in the cloud market has fallen steadily since 2017, dropping to around 13%. As noted by the European DIGITAL SME Alliance, just three US-based companies account for 65% of the European cloud services market — and are investing billions to extend that dominance. Big Tech has invested over $700 billion in AI infrastructure in 2025 alone, according to Euronews — all while repeating the same refrain: "Our servers are in Europe, you have nothing to fear." The following section explains precisely why this claim does not hold up.

A structural asymmetry is clearly identifiable today: the means mobilised in Europe are not remotely comparable in scale to those of the players across the Atlantic.

The Cloud Act and FISA: The Elephants in the Server Room

Beyond market share, it is the legal dimension that should alarm any decision-maker. The Cloud Act (2018) and Section 702 of FISA, along with its 2024 reform, allow US authorities to demand access to data stored by companies under their jurisdiction — including when that data is physically located in Europe.

This is not theoretical. In June 2025, The Register reported on a French Senate hearing where Microsoft France's director of public and legal affairs acknowledged that he could not guarantee that data of French citizens hosted on Microsoft servers located in France would never be transmitted to the US government without Paris's agreement. SDxCentral covered the same hearing in detail. This statement should appear in capital letters in every public tender involving an American hosting provider.

A legal analysis by activeMind.legal confirmed this risk: the location of data within the EU is not sufficient to guarantee its sovereignty when the provider is subject to US law. It is not geography that governs, but jurisdiction. Concretely, whether your data is stored in Paris, Frankfurt or Amsterdam, if it is hosted by a US provider, it is legally accessible to American intelligence agencies.

The GDPR requires that individuals be informed of access to their data and mandates transparency, while the FISA and the Cloud Act can impose such access under a veil of secrecy (gag orders), making even the reporting of that access impossible under the NIS2 directive. We are therefore in a Kafkaesque situation: data access mandated by US law can constitute a violation of European law, but US law prohibits reporting it. A frontal contradiction — and yet governments continue to sign contracts with these very providers.

Several sources and analyses confirm these facts:

- Section 504 of the FRRA / ECSP expansion in RISAA: clear analysis by ZwillGen law firm.
- Final text of the RISAA (H.R.7888)

The problem is not limited to cloud. The 2024 renewal of FISA and proposed reforms (Section 504 of the FRRA) could extend data disclosure obligations to equipment vendors, beyond cloud operators alone. The scope of the issue keeps expanding.

Extending the obligation to equipment vendors, beyond cloud operators

The new definition in RISAA now covers any "service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications."

Concretely, beyond cloud operators, this may include:

- Data centres / infrastructure hosting providers (colocation, housing) — even if they do not manage content.
- Managed service providers (MSP/MSSP) — IT outsourcing, network monitoring.
- Network and telecom equipment vendors — manufacturers/operators of routers, switches, firewalls (Cisco, Juniper, etc.).
- CDN (content delivery network) providers.
- IT maintenance contractors with physical or logical access to equipment.
- Wi-Fi access providers (explicitly mentioned in IRSEM analysis, though residential and restaurant Wi-Fi is excluded).
- SaaS software publishers hosting communications (messaging, videoconferencing, collaborative tools).

The IRSEM notes that the definition is considered "too broad" by the industry itself and that "simply providing a Wi-Fi connection" could theoretically fall within its scope.

For organisations wishing to align their practices with these legal realities, guidance on cybersecurity and sovereign infrastructure management can make the difference between theoretical compliance and effective protection.

European Initiatives That Need to Accelerate

No European country is alone in this endeavour. At EU level, an unprecedented regulatory arsenal is now operational. The DSA (Digital Services Act), fully applicable since February 2024, regulates online platforms to combat illegal content and enforce transparency — with a first fine of €120 million imposed on X in December 2025, and an investigation opened in January 2026 into its Grok chatbot.

The DMA (Digital Markets Act) targets "gatekeepers" and their anti-competitive practices, with new proceedings launched against Apple and Meta in April 2025 and new investigations against Google for opening Android to competing AI systems. The NIS2 directive strengthens cybersecurity obligations for critical infrastructure. And the Data Act, applicable since September 2025, governs access to data generated by connected devices, enforces cloud service interoperability and tackles the vendor lock-in practised by hyperscalers.

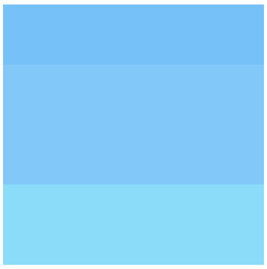
But these regulatory instruments have their limits. Fines imposed on Big Tech, even when they run into billions of euros, are absorbed as a cost of doing business: the DMA sanctions of April 2025 against Apple (€500M) and Meta (€200M) represented barely 0.5% of their annual profits. Geopolitical tensions are intensifying: Washington openly perceives the DSA and DMA as non-tariff barriers, with the Trump administration launching in December 2025 an official review of these regulations, which it considers "discriminatory" toward American champions.

Faced with these pressures, the Franco-German initiative marked a turning point. Announced in June 2025, formalised at the Toulon summit in August, it culminated on 18 November 2025 in the Berlin Summit on European Digital Sovereignty, co-chaired by President Macron and Chancellor

Merz before 900 decision-makers. The German Federal Government's official joint press release details the outcome: over €12 billion in private investment pledges, the launch of a Franco-German "Digital Sovereignty Task Force" tasked with defining sovereignty indicators for cloud, AI and cybersecurity (results expected at the 2026 Franco-German Council of Ministers), support for a Digital Commons European Digital Infrastructure Consortium (DC-EDIC) uniting France, Germany, the Netherlands and Italy, and — notably — the explicit recognition of open source as a strategic pillar, with Chancellor Merz revealing that the OpenDesk suite is already in use at the Federal Chancellery.

Encouraging signals. But the challenge remains as much cultural as political:
As long as European public and private decision-makers treat Big Tech as the "default" choice, no regulatory framework will be sufficient.

<?xml version="1.0" encoding="UTF-8"?>



GREEN LIGHT! 2013 ESR Act — Open Source Software first Art. L.123-4-1 — Education GREEN LIGHT! OUT OF FUEL!

2015 Microsoft Education Partnership — €13M Sponsorship — Free licences OUT OF FUEL! SPEED LIMIT! 50 2021 Cloud by Default Policy — DINUM Office deemed non-compliant SPEED LIMIT! STOP! STOP 2022 Office 365 & Google banned — Schools Latombe Parliamentary Question STOP! ACCIDENT! MARCH 2025 Microsoft Framework Agreement €152M 4 years — no competitive tender ACCIDENT! FLAT TYRE! MARCH 2025 École Polytechnique → Microsoft 365 Defence data exposed FLAT TYRE! FUEL!

JUNE 2025 Cabinet Council on Digital Sovereignty €264Bn/yr dependency FUEL! PUNCTURE-PROOF! ★ 2024 GendBuntu — 97% 103,164 Linux workstations SECRET WEAPON PUNCTURE-PROOF! ROLL! JAN 2026 Digital Sovereignty Observatory Clément Beaune ROLL! © 2026 OpenSourceSolutions.pro — Inspired by the Mille Bornes® card game

Education Systems: Unwitting Factories of Big Tech Dependency

A Field Riddled with Contradictions

If governments' digital dependency is worrying, that of education systems is truly dizzying — and far heavier in long-term consequences. Because schools do not merely use tools: they shape habits, reflexes, and cognitive dependencies.

The issue is not new. The Free Software Foundation Europe (FSFE) has long campaigned for free software in education, warning that every student and teacher obliged to hold a Microsoft or Google account creates "a lasting dependency." As early as 2015, a partnership between the French Education Ministry and Microsoft triggered an outcry from free software associations and teachers' unions for exactly this reason.

In 2022, the French Ministry of Education officially requested a halt to the deployment of Office 365 and Google Workspace in schools, on the grounds that these solutions are neither GDPR-compliant nor consistent with the cloud-first doctrine. France's CNIL data protection authority recommended the use of collaborative suites hosted in the EU by providers subject exclusively to European law. At European level, the European Data Protection Supervisor (EDPS) opened investigations in 2021 into the use of Microsoft services by EU institutions themselves, highlighting the structural nature of the problem. Three years after the French Ministry's directive, the situation on the ground tells a different story.

March 2025: The Renewal That Called Everything into Question

On 14 March 2025, a notice published in the French Official Bulletin revealed the award of a four-year framework agreement for Microsoft licences worth up to €152 million. In the middle of a period of transatlantic tensions, at the very moment when the government was multiplying its speeches on digital sovereignty, the Education Ministry was renewing its Microsoft "open bar."

The FSFE's "Public Money? Public Code!" campaign has long argued that this amounts to a form of dumping and unfair competition: no competitive tender is launched for free offers, which mechanically eliminates European competitors. A deputy in the French National Assembly demanded the Ministry denounce the contract, recalling that the DINUM circular prohibits the deployment of Office 365 in French administrations.

Concurrently, the leadership of École polytechnique — a flagship institution under the Ministry of Defence, whose research feeds into our most critical sectors (military, cyber, quantum) — decided, without consultation, to migrate its data to Microsoft 365, raising serious concerns about the security of sensitive research data, including data relevant to national security.

The irony is bitter: the same state that creates a Digital Sovereignty Observatory is simultaneously funding, with public money, a deepening of its dependence on Microsoft.

Free Offers as a Trojan Horse

The mechanism is well-established. Microsoft and Google offer "free" solutions to educational institutions — Office 365 for the former, Google Workspace for Education for the latter. This generosity is obviously not disinterested. It amounts to a form of dumping and unfair competition: no competitive tender is launched for free offers, which mechanically eliminates European competitors.

The effect is systemic and perfectly calculated. A student who uses Word and Excel throughout thirteen years of schooling will not spontaneously consider LibreOffice in the workplace. A teacher trained on Google Classroom will not voluntarily migrate to Moodle. The initial free offer transforms into a dependency rent: personal licences, cloud subscriptions, Microsoft or Google professional certifications. The entire downstream commercial ecosystem benefits from this early conditioning.

In marketing terms, this is a "land and expand" strategy applied to a captive audience of minors. School becomes the first link in a lock-in chain that continues through higher education, professional life, and into personal usage.

And what of the data? Information collected throughout a student's schooling — grades, behaviour, absences, skills acquired or not, parental involvement, disabilities — constitutes a detailed profile of millions of minors, accumulated over at least thirteen years.

Things do shift sometimes. Let us be concrete and give tangible examples.
Solutions like Pronote (Index Éducation, hosting certified to the highest French sovereign standard on a proprietary French datacentre) or Germany's Moodle-based deployments show that it is perfectly possible to manage school life with sovereign European solutions. But these school management tools coexist daily with American office and collaboration suites — students and teachers share work in Google Drive, teachers organise videoconferences in Teams, and Chromebook or iPad tablets are deployed en masse.

The sovereignty of management tools masks the dependency of pedagogical tools — even though the alternative model already exists, and we will discuss it now.

Alternatives Exist — and They Work

The claim that no credible alternative to Big Tech exists in education is factually false.

France's Interministerial Free Software Catalogue (SILL), maintained by the DINUM, currently references more than 530 mature solutions for every use case: LibreOffice for office productivity, Tiki Wiki for collaboration and content management, Nextcloud for file sharing, Moodle for LMS, Thunderbird or Tiki Wiki for messaging, Jitsi Meet for videoconferencing — and right down to infrastructure tools: server management, monitoring, web traffic analytics. The entire technical stack has proven open source equivalents in production use. At EU level, the European Commission's Joinup platform catalogues hundreds of reusable public sector solutions.

Certified European hosting providers — OVHcloud, Hetzner, IONOS — can accommodate educational data within a legally secure framework, protected from American extraterritorial laws. The estimated 15–20% cost premium compared to hyperscalers is the price of sovereignty, but it is an investment in independence, not superfluous expenditure.

The French Gendarmerie nationale has shown the way at scale. Since 2008, it has progressively migrated its entire fleet, reaching 97% of 103,000+ workstations running GendBuntu by June 2024 using its own Ubuntu-based distribution with LibreOffice, Firefox and Thunderbird. The result: recurring savings on over 700,000 licences and a reduction in total cost of ownership of around 40%, without impact on operational productivity. Munich's LiMux project — despite its politically complicated ending — similarly demonstrated that large-scale migration to Linux in public administration is technically viable.

A determined policy would make it possible to generalise mature open source solutions such as Tiki Wiki, Odoo or Moodle, to draw on the Comptoir du Libre catalogue by ADULLACT, to deploy the tools of LaSuite Numérique (France) or OpenDesk (Germany/EU), and more broadly to mobilise a rich ecosystem of free and sovereign solutions. What is missing is a structured network of public open source digital advisors capable of guiding every school, municipality, museum and institution toward sovereign, interoperable, locally hosted solutions — supporting a fabric of local open source service providers.

And the legal texts already provide for this. The FSFE's "Public Money? Public Code!" campaign calls on European legislators to require publicly funded software to be released as free software. In France, the Higher Education and Research Act of 2013 requires that "free software be used in priority" in public higher education. The Digital Republic Act of 2016 encourages the use of free software across the entire public sector. These texts exist. They are simply ignored.

Training for Sovereignty, Not Just for the Tool

The educational challenge goes beyond software choices. It is digital culture itself that must be rethought. Teaching a student to use Word is training a consumer. Teaching them to understand what a file format is, why interoperability matters, how personal data works — that is training a citizen.

According to the OECD's TALIS 2018 survey, only 34% of primary school teachers had taken part in digital training in the previous year. This deficit is an opportunity: training educators not on a specific commercial product, but on cross-cutting competences and open tools, is an investment in long-term autonomy.

The European Erasmus+ programme and the Digital Education Action Plan 2021–2027 already support this vision. The European Schoolnet Academy offers free teacher training on digital skills and open educational resources. Initiatives fostering critical thinking on disinformation show that it is possible to teach about the digital world without submitting to the platforms that monopolise access to it.

To engage in this transition, institutions and organisations can rely on specialised actors. Open Source Solutions is one of them and offers |structured technical support in digital sovereignty, from audit to migration toward free and sovereign solutions, enabling organisations to turn intention into operational reality.

A Call for Coherence

Digital sovereignty cannot be a morning ambition and an afternoon contradiction. One cannot create a Digital Sovereignty Observatory in January 2026 and have signed a €152 million Microsoft framework agreement ten months earlier. One cannot ban Office 365 in administrations and fund it in schools. One cannot legislate on data protection while entrusting the data of millions of pupils to companies subject to the Cloud Act.

Coherence is not a luxury. It is the prerequisite for credibility. And that credibility will determine whether Europe manages to turn its ambitions into real infrastructure — or whether it continues to write roadmaps on American servers.

The various sovereignty observatories and task forces launched across Europe must deliver concrete analyses in 2026. They could represent a turning point — provided their conclusions translate into concrete public procurement decisions, into exclusion criteria in sensitive tenders, and into migration roadmaps for the most dependent administrations. Above all, this coherence must apply from start to finish of the chain: companies and individual users must be included in this march toward digital autonomy.

The tools exist.
The skills exist.
The legal frameworks exist.
What is missing is the will to move from words to deeds — decision by decision, public contract by public contract, classroom by classroom. Making digital education the starting point for breaking dependency is to recognise that sovereignty is built from the earliest age.

In our third and (likely) final article in this series, we will address concrete solutions at the organisational level. We will detail how an SME, a local authority or an institution can, starting today, regain control of its digital infrastructure by drawing on sovereign and operational alternatives.