LOTEC

Operationalizing Digital Sovereignty

A due-diligence framework for European digital autonomy.

Stefane Fermigier — CEO Abilian, co-chair CNLL & APELL, co-founder EuroStack Initiative

(Sambruk 2026)

About Me

Stefane Fermigier

- Free software entrepreneur since 2000 (Linbox, Nuxeo, Abilian).
- Creator of free software (Hop3: cloud self-hosting platform, Abilian SBE: open source digital workplace ...).
- Co-chair of **CNLL** & **APELL** (French and EU open source industry federations).
- Co-founder of the **EuroStack Initiative Foundation e.V.**
- Member of the French "Numérique de Confiance" strategic committee.

Perspective

- This talk is not about compliance or cybersecurity — it is about the **strategic and industrial consequences** of public procurement choices.
- Thesis: facing hyperscaler network effects,
  - Europe must aggressively protect its digital industry;
  - Open Source is the strongest lever for Europe's technological catch-up.

Part 1

The Diagnosis — A Digital Colony

The Economic Hemorrhage

Europe is massively funding the development of its competitors.

- **€265 billion/year** flow from the EU to US suppliers (just for cloud and B2B software!).
- That is roughly **80%** of European enterprise software spend.
- It is a structural **transfer of wealth**.
- We are draining our own innovation ecosystem.

Digital sovereignty is the strategic autonomy of an entire continent.
It concerns public bodies, but also companies and citizens.

Value Extraction

The dominant business model: capture the European market, repatriate the profits.

Extortionate practices of dominant vendors:

- **Microsoft** — arbitrary price hikes (+15-20%/year on M365), forced bundling.
- **VMware/Broadcom** — 3-5x cost increases after acquisition, end of perpetual licenses.
- **Oracle** — aggressive audits, punitive cloud licensing.
- **Egress fees** — a tax on the freedom to leave.

Once you are locked in, the vendor sets the price.

The Geopolitical Risk

Sovereignty is not about betting on the goodwill of allies.

The "kill switch" is real:

- **Adobe in Venezuela (2019)** — accounts shut down overnight by US executive order.
- **Microsoft vs ICC (2025)** — International Criminal Court Chief Prosecutor's email cut under US sanctions.
- **Technology sanctions** — Huawei (2019), Russia (2022), ongoing restrictions on updates, APIs, cloud services.
- **FISA 702 (reauthorized 2024) / CLOUD Act (2018)** — access to data even when hosted in Europe.

Strategic autonomy is also the ability to say "no".

Regulation Alone Is Not Enough

Europe is the "world champion of regulation": GDPR, DMA, DSA, AI Act, CRA ...

But **"Code is Law"** (Lawrence Lessig).

- If we do not own the infrastructure, our laws only apply when the owner allows it.
- GDPR protects personal data but does not neutralize extraterritoriality.
- NIS2 secures networks but ignores the nationality of the supplier.
- EUCS was stripped of its sovereignty criteria under lobby pressure.

We must shift from regulating to building.

Part 2

Beyond Data Residency

The Sovereign Prison (aka "Sovereignty-Washing")

Do not confuse **data residency** with **sovereignty**.

The trap:

- Data stored in Europe — check.
- But "black box" technology.
- Controlled from abroad.
- Proprietary, non-auditable code.
- Technical and contractual lock-in.

The consequences:

- Price hikes with no recourse.
- Migration becomes prohibitively expensive.
- Dependency on the vendor's roadmap.
- No real security audit possible.
- No resilience.

Your data is there, but you have no freedom of action.

What We Are Actually After: Optionality

The goal is not autarky. It is **optionality**.

What we want:

- the **choice** to switch supplier.
- partnership **as equals**.
- interdependence, not unilateral dependency.
- the ability to federate existing assets.

What it requires:

- credible alternatives.
- open standards and/or open source.
- a mastered supply chain.
- a viable industrial ecosystem.

"Stay by choice, not by constraint."

Part 3

The LOTEC Framework

Legal · **O**perational · **T**echnological · **E**conomic · **C**ultural

LOTEC: A Holistic Due-Diligence Grid

Facing marketing confusion, a **5-pillar** framework:

Criterion	Central question
L – Legal	Which jurisdiction are you ultimately subject to?
O – Operational	Who effectively controls the infrastructure?
T – Technological	What technical mastery and reversibility?
E – Economic	Where is value created and captured?
C – Cultural	Are we building the skills and mindset to stay in control?

Without objective criteria, "sovereign" means nothing.

[L] Legal – Jurisdictional Immunity

Concept: legal immunity vs. apparent compliance.

> If a foreign court (FISA, Cloud Act) demands your data, can your supplier legally refuse?

If the parent company is outside the EU:

- the answer is **no**.
- the GDPR contract does not protect you.
- foreign law overrides the contract.

Key criteria:

- ultimate parent of the control chain in the EU.
- more than 50% of voting rights held in the EU.
- no non-EU "blocking minority".
- IP not subject to foreign export control.

Legal immunity is a must-have – but addressing only this pillar leads to "sovereignty washing".

[O] Operational — Effective Control

Concept: who holds the keys to the truck?

Having servers in Stockholm is not enough if the **control plane** is driven from Seattle.

Key criteria:

- **Infrastructure** — datacenters and networks on European soil.
- **Control plane** — admin console operated from the EU.
- **Personnel** — 100% of privileged (root/admin) access held by EU residents, employed by an EU entity.
- **Supply chain** — documented strategy to reduce critical dependencies.
- **Security** — robust encryption, NIS2 compliance, documented incident procedures.

An admin in Seattle can be legally compelled by US authorities.

[T] Technological — Transparency and Reversibility

Warning: open source ≠ open standards. They are interelated, and both are needed.

Open standards ("enforceable"):

- interoperability guarantee.
- data and workload portability.
- no royalties or blocking patents.
- multiple implementations possible.

Open source:

- auditable code (no backdoors).
- fork possible when needed (ex: Euro-Office last week)
- independent verification (reproducibility).
- caveat: governance is sometimes US-based (e.g. Linux Foundation ...) and/or tied to (US and Chinese) Big-Tech.

Reversibility: full documentation, contractual exit plan, no punitive egress fees.

[E] Economic — Value Capture

Concept: where does the money go? Who benefits from the growth?

Value creation criteria:

- more than 50% of global R&D in Europe.
- skilled local jobs.
- European intellectual property.
- profits reinvested in the EU.
- partnerships with European firms and academia.

Pitfalls to anticipate and avoid:

- punitive egress fees.
- tied-selling and forced bundling.
- aggressive licensing audits.
- unilateral end of perpetual licenses.

"If I pay a license, am I funding engineers in Berlin or in California?"

[C] Cultural — Competencies and Mindset

Concept: sovereignty is ultimately a matter of **people (skills and mindsets)**, not just contracts and servers.

Build the skills:

- IT staff trained on European and open source stacks, not just vendor certifications.
- procurement officers able to write reversibility and immunity clauses.
- open source in engineering curricula; sovereignty issues in secondary school.

Participate actively:

- contribute to open source projects critical to Europe — don't just consume them.
- engage in standards bodies and governance rather than leaving them to Big-Tech.
- host foundations and consortia under EU or neutral law (cf. RISC-V moving to Switzerland).

Two traps to break:

- the "nobody got fired for buying from Big-Tech" default,
- Europe funding its own lock-in — "free" vendor training, EU startups funded to run on US cloud.

Part 4

Related Frameworks (from EuroStack and the Commission)

EuroStack – The JOTED Framework

Published by the EuroStack Industrial Initiative in late 2025.

Structure in 5 dimensions: Jurisdiction, Operations, Technology, Economic, Data.

Major specificity: the **jurisdictional** criterion is a **pass/fail gate**.

Hierarchy of evaluation:

1. **Level 1 – Jurisdiction** (eliminatory): EU headquarters, majority EU voting rights, immunity from FISA/CLOUD Act.
2. **Level 2 – Core guarantees** (Ops, Tech, Data): control plane in the EU, open source and open standards, strict data residency, customer-managed keys.
3. **Level 3 – Economic differentiator**: local R&D (>50%), contribution to the European open source ecosystem.

LOTEC defines the pillars; JOTED and CSF operationalize them. JOTED's distinctive choice: jurisdiction as a hard pass/fail gate, with a clear hierarchy of evaluation. CSF (next slide) makes different design choices.

The Cloud Sovereignty Framework (EC)

A methodology for public procurement (v1.2.1, October 2025).

- **SEAL** = *Sovereignty Effectiveness Assurance Level* — 0 to 4, used as an **exclusionary prerequisite**.
- **SOV** = *Sovereignty Objective* — 8 weighted criteria used to **score** compliant offers.

Two-step approach: minimum SEAL level first, then a weighted score across the 8 SOVs:

- **Supply chain** — 20%
- **Strategic**, **Operations**, **Technology** — 15% each
- **Legal**, **Data**, **Security** — 10% each
- **Environment** — 5%

Major weakness: the scoring formula and applicability rules are currently **opaque** — how sub-criteria aggregate, which procurements are covered, and how each objective is actually measured all remain unclear. Wide room for "sovereignty washing".

Part 5

Putting LOTEC to Work

Risk-Based Arbitrage

Do not chase "100% sovereign" for everything. Make a **risk-informed** decision.

Critical data *(health, R&D, citizens, defense)*

Non-negotiable on:

- **L** (Legal) — hard requirement.
- **O** (Operational) — full control.
- **T** (Technological) — guaranteed reversibility.

Less sensitive data *(public website, marketing analytics)*

Trade-offs possible:

- **L** more flexible if data is non-critical.
- focus on **T** (performance, features).
- but always evaluate **E** (hidden costs).

The point: decide deliberately, not by default.

Public Procurement – The Major Lever

Public procurement is not just an operating expense. It is an **industrial investment**.

The action:

- embed LOTEC criteria (or similar) in tender specifications.
- target **20-30%** of budgets toward solutions with strong European value creation.
- use security exceptions (Art. 346 TFEU, Art. III GPA/WTO).

The impact:

- creates a viable market for European SMEs.
- scale effect: from niche to mainstream.
- strong political signal.
- local skills development.

"Public money, public code. Open source priority. European preference."

Call to Action

Digital sovereignty is not decreed. It is built **project by project**.

For CIOs and architects:

- map your critical dependencies.
- evaluate them against the LOTEC or similar grids.
- identify the legal "single points of failure".

For economic and political decision-makers:

- embed sovereignty criteria in procurement.
- support the European ecosystem (including SMEs, open source).
- demand transparency from your suppliers.

"Do not build your digital future on land you do not own."

Conclusion

The year 2025 marked the end of technological naivety.

The challenge is not (only) legal, it is industrial.

We have the talent. We have the internal market. What is missing is the strategic alignment to **build** rather than buy.

Open source is the key.
It is the main lever to transform IT spending into asset investment.

Resources

Initiatives and associations:

- **EuroStack Foundation** — eurostack.eu
- **APELL** — apell.info

Practical tools:

- **EuroStack Directory** — euro-stack.com (European solutions catalog).
- **SILL** — code.gouv.fr/sill (French public sector OSS catalog).
- **IRN** — resiliencenumerique.com (Digital Resilience Index).

Contact: sf@abilian.com / sf@fermigier.com

Thank you. Questions?