

Trend topic: **Sovereignty**

By



Dr. Konstantinos Komaitis

Resident Senior Fellow,
Digital Forensic Research Lab,
Tech and Democracy Initiative
at the Atlantic Council

Dr. Komaitis currently serves as a Senior Resident Fellow at the Atlantic Council's Democracy and Tech Initiative, where he leads efforts in digital governance and democracy. Previously, he spent nearly a decade at the Internet Society as the Director of Policy Development and Strategy, navigating complex global regulatory landscapes. He also spent time at The New York Times, where his work focused on critical issues of data governance.

Explore more from
The Kyndryl Institute
kyndryl.com/institute

Europe's digital sovereignty debate needs more infrastructure realism

For years, digital sovereignty was largely a Brussels phrase: politically useful, strategically vague, and easy to invoke. That is no longer the case, as today, it is shaping boardroom conversations¹ across Europe.

That shift is understandable. A decade of supply chain disruption, cyberattacks, geopolitical instability and regulatory divergence has exposed how deeply Europe depends on infrastructure, platforms and suppliers beyond its direct control. For instance, as of 2025², while over 52% of EU enterprises have adopted paid cloud services, more than 77% of those users are now classified as 'highly dependent' on sophisticated cloud stacks—the vast majority of which are provided by non-EU hyperscalers. For businesses that dependency is no longer abstract, and it raises practical questions about resilience, legal exposure, continuity and trust.

Europe is right to want greater control over its digital future. But there is a growing risk in how the debate is evolving. Too much of the conversation still treats sovereignty as if it were primarily a matter of location: where data is stored, where a cloud provider is headquartered, or whether a supplier is European or non-European. Those questions matter but they are not sufficient. In critical systems, control is not determined by geography,

security is not guaranteed by ownership, and resilience is not created by building digital walls.

If Europe wants a serious digital sovereignty agenda, it needs to move beyond symbolism and confront the operational reality of modern infrastructure. The central question is not whether Europe can become digitally independent in any pure sense. It cannot. The real question is whether Europe can become more resilient, more governable and less strategically exposed within a deeply interconnected digital economy. That is the test that matters.

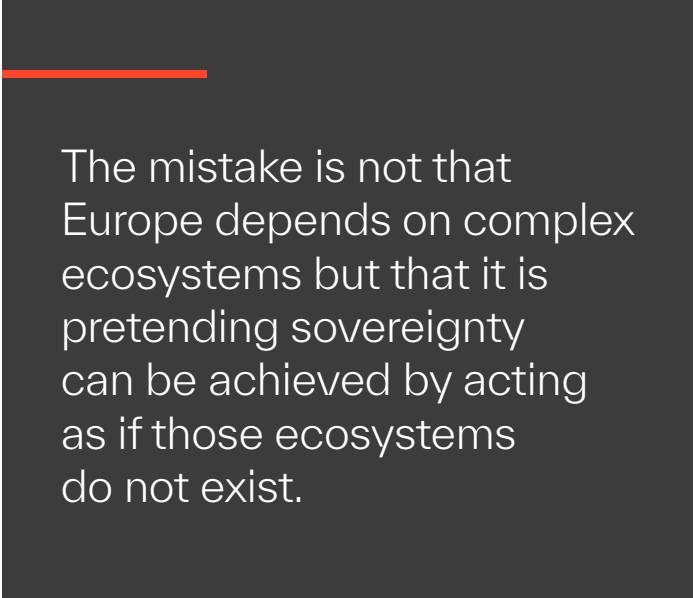
A simple way to cut through the rhetoric is to ask what digital sovereignty means when you are responsible for keeping a critical service running.

Consider a large European bank. It may strongly support the idea of greater digital sovereignty, but it cannot support a version of sovereignty that makes payment systems less reliable, fraud detection slower, cyber response weaker or customer services harder to recover during disruption. Its customers do not care whether sovereignty looks elegant on paper; they care whether payments clear, digital channels stay online and their data remains protected under stress.

The same logic applies well beyond financial services. Hospitals need clinical systems to remain available. Manufacturers need production lines to keep moving. Energy operators need grid systems to stay stable. Logistics providers need supply chains to keep flowing. Governments need public services to function during crisis. In each case, sovereignty is not a philosophical concept but an operational one.

That distinction matters because much of the current debate still implies that control can be created through exclusion, by repatriating workloads, favoring local suppliers, or narrowing access to a smaller set of “acceptable” providers. In some cases, those choices may be justified. But when treated as an end in themselves, they can produce exactly the opposite: less resilience, more concentration risk and greater fragility. The 2021 fire at the OVHcloud data center in Strasbourg serves as a stark reminder³;

thousands of European entities that had localized their data with a single 'sovereign' provider found themselves without backups or contingency, proving that geographic proximity is no substitute for architectural redundancy.



The mistake is not that Europe depends on complex ecosystems but that it is pretending sovereignty can be achieved by acting as if those ecosystems do not exist.

The uncomfortable truth is that no major enterprise or government in Europe operates inside a sealed national or continental technology stack. Modern infrastructure is layered across legacy systems, private clouds, public clouds, colocation facilities, telecom networks, software platforms, identity services, cybersecurity tooling, semiconductor supply chains and globally distributed support models. Software updates, access controls, threat intelligence, monitoring and incident response routinely cross jurisdictions. Even services that appear local often depend on globally sourced components somewhere in the stack.

This is not a flaw in the system. It is the system.

The mistake is not that Europe depends on complex ecosystems but that it is pretending sovereignty can be achieved by acting as if those ecosystems do not exist. This is why any serious digital sovereignty strategy should be judged through three tests: whether it improves resilience, whether it preserves interoperability and whether it maintains openness.



Resilience comes first because sovereignty without continuity is meaningless. A system that cannot absorb outages, cyberattacks, supplier failures or geopolitical shocks is not sovereign in any practical sense. This is particularly relevant in Europe, where many critical environments still run across aging networks, fragmented application estates and under-invested operational infrastructure. In those environments, adding sovereignty requirements on top of existing fragility can increase risk rather than reduce it.

Interoperability is the second and arguably most overlooked condition of sovereignty. If digital sovereignty leads Europe toward closed architectures, bespoke local stacks or technically incompatible environments, it will reduce flexibility at exactly the moment flexibility matters most. Interoperability is what allows organizations to avoid lock-in, diversify suppliers, move workloads when risk changes, integrate security controls across hybrid environments and maintain continuity when one part of the stack fails. In that sense, interoperability is not the enemy of sovereignty but one of its preconditions.

Europe should be deeply skeptical of sovereignty models that produce fragmentation in the name of control. Open standards, API-led integration, modular platforms and architectures designed for portability should be treated as strategic assets, not

technical preferences. Equally important is resisting the temptation to let different countries, sectors or regulators define sovereignty so differently that the single market fractures into incompatible digital regimes. A sovereignty agenda that undermines interoperability will not strengthen Europe but reduce its room to maneuver.

Openness is the third test, and perhaps the most counterintuitive in this debate. Yet Europe's strength has historically come from combining strong rules, trusted institutions and open markets. The same should be true digitally.

Openness does not mean complacency about dependency; nor does it mean ignoring lawful access concerns, cyber exposure or strategic vulnerabilities. It means recognizing that innovation, scale, ecosystem diversity and competitive pressure are themselves sources of resilience. This is where one of the least discussed risks in the current debate becomes especially important: concentration disguised as control.

If Europe tries to reduce reliance on a handful of global providers by moving too quickly into a narrow pool of regional alternatives, it may simply replace one concentration risk with another, and potentially a more dangerous one. The alternative may offer less geographic redundancy, smaller cyber operations,

Europe should absolutely invest in strategic digital capacity but leaders need to distinguish between building optionality and mandating enclosure. One expands resilience. The other can shrink it.

weaker supply chain depth or less mature incident response capabilities. In other words, “more local” does not automatically mean “more secure.”

That is not an argument against European capability. Europe should absolutely invest in strategic digital capacity but leaders need to distinguish between building optionality and mandating enclosure. One expands resilience. The other can shrink it.

Much of the public debate still overemphasizes data residency and underplays the operational risks that actually determine control. Fragmentation is one of them. If every regulator, country or sector defines sovereignty differently, organizations will be pushed into customized architectures that are harder to secure, harder to audit and harder to recover. False assurance is another. Local hosting can create the appearance of control while leaving unresolved the more difficult issues of privileged access, software supply chain exposure, identity weakness, observability gaps, lawful access conflicts and poor recovery design. Poorly sequenced change may be the most immediate risk of all. If sovereignty becomes a trigger for rushed migrations or politically driven platform decisions, organizations may reduce security in the name of improving it.

So what is feasible?

Not wholesale repatriation; not “European-only” stacks; and, not symbolic redesigns that ignore how critical systems actually operate.

The more credible path is selective, risk-based redesign of critical infrastructure. Sensitive workloads can be segmented according to risk and policy rather than ideology. Encryption keys and trust services can be structured so that control remains with the customer or within the region where appropriate. Privileged access can be narrowed and continuously monitored. Observability can be strengthened across hybrid and multi-provider environments. Recovery and failover models can be redesigned to reduce dependency on any single operator, provider or jurisdiction. Contracts can be modernized to support auditability, portability and meaningful exit options. And platforms can be designed so that switching is technically possible, not just legally imaginable. The real objective is not to isolate infrastructure from the world; it is to govern complexity well enough that critical systems remain trusted, secure and operational even as the world becomes more volatile. In that sense, digital sovereignty should be measured less by how “local” infrastructure appears and more by whether it remains resilient under stress, interoperable across environments, open enough to preserve innovation and optionality, and governable when disruption hits.

That is not a compromise position. It is the only version of digital sovereignty that can survive contact with operational reality. —

References

- 1 Digital autonomy: Achieve technology sovereignty today | McKinsey
- 2 37043.pdf
- 3 The OVHCloud Dumpster Fire (literally and figuratively) - Backup Central