European Sovereignty Grows Up for the AI Age

For several years, European technology sovereignty was often discussed as an aspiration: Europe should control its data, reduce reliance on foreign technology and develop credible alternatives to the dominant global platforms. The objective was understandable but the term itself remained imprecise. Sovereignty could mean anything from storing data in an EU data centre to requiring European ownership of an entire technology stack.

The European Commission's new Technological Sovereignty Package (European Commission) suggests that this thinking is beginning to mature. Presented on 3 June 2026, the package combines proposed measures covering semiconductors, cloud and AI infrastructure, open-source software, and the digitalisation of energy. It represents an acknowledgement that sovereignty cannot be achieved through regulation alone. Europe must also possess the infrastructure, industrial capability, skills and market demand needed to exercise meaningful technological choice.

In this brief I provide a synthesis of the EU's evolved position and place this into real world context.

From technological independence to practical control

The most important development is a more practical definition of sovereignty.

Sovereignty does not necessarily require every chip, model, cloud platform or software component to be European. In a globally interconnected technology economy, absolute self-sufficiency would be prohibitively expensive, slow and potentially counterproductive.

Instead, sovereignty is increasingly being framed as the ability to make, enforce and preserve European choices.

That means being able to determine:

- who controls sensitive data and encryption keys;
- which jurisdiction governs the service;
- who can administer, modify or suspend the platform;
- where critical software, hardware and operational dependencies originate;
- whether workloads can be moved or recovered;
- whether the service can continue during geopolitical, commercial or supply-chain disruption;
- and whether compliance with European law can be independently demonstrated.

The Commission's Cloud Sovereignty Framework illustrates this shift. It translates sovereignty into measurable procurement criteria covering strategic control, jurisdiction, data and AI, operations, supply chains, technology, security, compliance and sustainability. Sovereignty is therefore no longer treated simply as a claim made by a supplier. It becomes a set of characteristics that can be assessed, scored and contractually required. This is a much more useful model for the AI era.

Sovereignty in an AI era moving at machine speed

AI changes the sovereignty debate because technological dependency is no longer static.

Cloud platforms used to evolve through relatively predictable product and infrastructure cycles. AI platforms can now change materially within months. Models are replaced, inference architectures evolve, new accelerator generations emerge, agent frameworks proliferate and proprietary interfaces become embedded throughout organisational processes.

A sovereign position established today can therefore erode quickly and adapts in real-time not to governance, compliance or risk management static timeframes.

An organisation may retain legal ownership of its data while becoming operationally dependent upon a foreign foundation model. It may use a European cloud provider whose critical control plane, update process or semiconductor supply chain remains externally controlled. It may deploy an open-source model but rely upon proprietary accelerators, libraries, orchestration platforms or remote management services. Sovereignty must consequently be treated as a continuing capability rather than a one-off certification.

The practical question is no longer simply *"Where is the data?"*

It is *"Who retains effective authority over the complete system and what happens when a dependency changes, fails or is withdrawn?"*

Why this matters

This more realistic definition is important for three reasons.

First, it connects sovereignty with resilience. Dependency is not inherently unacceptable but dependency without alternatives, visibility or recovery options becomes a strategic vulnerability.

Second, it connects sovereignty with competitiveness. Europe cannot regulate its way to AI leadership while depending overwhelmingly on external providers for advanced chips, cloud infrastructure, foundational models and software platforms. The EU's own Digital Decade assessment (Digital Strategy) acknowledges that significant dependencies remain in semiconductors, cloud and cybersecurity and that is not going to change anytime soon.

Third, it connects sovereignty with commercial leverage. When public sector and regulated industry procurement includes measurable sovereignty requirements, providers have a financial incentive to offer stronger jurisdictional protections, operational separation, supply-chain transparency, interoperability and exit arrangements.

Sovereignty thereby moves from political rhetoric into architecture, procurement and contract management.

The challenge for organisations

The danger is that organisations interpret the new direction too simplistically.

Moving workloads to a European data centre does not automatically create sovereignty. Neither does contracting with a European reseller, adopting open source or selecting a provider with 'sovereign' in its product name.

Organisations will need to examine the full dependency chain from ownership, governance, administrators, source code, binaries, model weights, training and inference data, software updates, telemetry, identity services, cryptographic keys, hardware, support arrangements, subcontractors and so on ...

They must also avoid creating sovereignty programmes that inhibit innovation. Excessively rigid localisation or European origin requirements could reduce access to the best available technology,

increase costs and leave organisations operating outdated platforms. In an era of exponential AI development and innovation event horizons, technological isolation may itself become a resilience risk as well a competitive Achillies heel.

There is also a danger of sovereignty theatre. That of elaborate questionnaires, labels and contractual statements that provide little evidence of genuine operational independence. Think tick box compliance as well. A provider may satisfy formal ownership requirements while remaining dependent on another company for its control plane, source code, security updates or specialist engineering capability.

Exit plans present another challenge. Many organisations state that they can change providers but have never tested whether applications, models, data, identities and operational processes can be transferred within an acceptable time and cost. Untested portability is not sovereignty; it is optimism. Analogous to Oracle lock-in in the 1990s, VMware in the 2000s and hyperscaler in the 2010s+ amongst others, painful, expensive experiences and in some cases, extinction born of rigidity when agility was key.

A more adaptive model

Organisations should therefore treat sovereignty as a risk-based and continuously managed position.

Critical national infrastructure, defence, healthcare and highly sensitive government workloads may require extensive European control and operational autonomy. Less sensitive commercial workloads may appropriately use global platforms, provided that jurisdictional, concentration and continuity risks are understood.

The objective should not be to eliminate every external dependency. It should be to prevent any dependency from silently becoming an irreversible point of control.

The key will be the shift to a real time, evergreen and on demand cyber security business operating model, that looks beyond the obvious, evolve established ways of thinking, reappraise old assumptions, finds new answers to not just harness the potential of an AI world but for many it's about avoiding extinction.

For more on the real-time demand theme see *'AI Has Not Changed the Rules … It Has Changed Whether Governance & Risk Management Can Keep Up'*

Conclusion

The EU's emerging approach reflects a welcome adaptation to the realities of AI. Sovereignty is becoming less about technological nationality and more about demonstrable authority, resilience, transparency and choice.

That is the right direction. In a fast-moving AI economy, the EU will not remain sovereign by attempting to freeze technology at the border. It will do so by ensuring that European governments and organisations can adopt global innovation without surrendering the practical ability to govern, secure, change or continue the systems on which they depend.

END