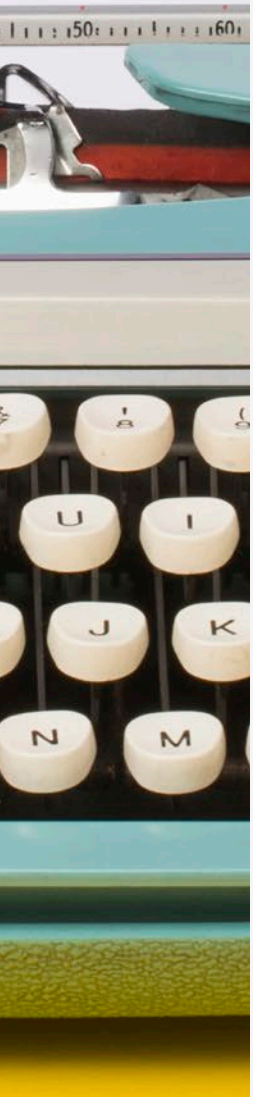
sogeti labs
Part of Capgemini

Access Denied

Report 3 of the **Autopilot** series

Table of contents

Introduction: Access Denied



There was no outage, no cyberattack, no visible malfunction. The systems themselves continued to operate exactly as designed. And yet, access stopped working.

On 6 February 2025, an executive order 14203[1] issued by the United States government introduced sanctions affecting the International Criminal Court (ICC). The measure was part of a broader legal and diplomatic response to developments surrounding the court's investigations regarding the war in Gaza. As with any such decision, it triggered a chain of compliance obligations across organisations operating under that jurisdiction.

As part of the compliance process, access to digital services used by the ICC was restricted. In a widely reported case,[2] the court's chief prosecutor Karim Khan found himself locked out of his email, documents and communication systems. Services hosted on external platforms. No systems had failed. No infrastructure had been compromised. But access had become conditional. What appeared on the screen was simple and unambiguous: **Access Denied**.

Although later news reports[3] and statements by the service provider nuanced the course of events, the incident revealed something much larger and fundamental. Microsoft, through its president Brad Smith, stated that it did not suspend or terminate services to the International Criminal Court (ICC). Instead, the company maintained that only the account of the sanctioned individual (Karim Khan) was disconnected as part of compliance processes, while all services to the ICC as an organisation remained fully operational.

---

[1] Donald J. Trump (2nd Term). (2025, February 6). *Executive Order 14203—Imposing Sanctions on the International Criminal Court*. The American Presidency Project. https://www.presidency.ucsb.edu/documents/executive-order-14203-imposing-sanctions-the-international-criminal-court

[2] Quell, M. (2025, May 15). *Trump's sanctions on ICC prosecutor have halted tribunal's work*. Associated Press. https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

[3] Clark, S. (2025, June 4). *Microsoft didn't cut services to International Criminal Court, its president says.* Politico. https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/

Microsoft emphasized that it stayed in contact with the ICC throughout and framed the action as a targeted, account-level measure rather than a broader service shutdown, while declining to provide detailed transparency on the exact mechanism behind the disconnection.

For decades, digital infrastructure has been treated as neutral ground. Cloud platforms, software services, and data flows formed the invisible backbone of modern organisations – reliable, scalable, and largely taken for granted. Technology was something we used, not something we questioned.

That assumption is beginning to shift. As digital systems have become more deeply embedded in how organisations operate, they have also become more closely intertwined with the environments in which they exist – legal frameworks, regulatory obligations and broader geopolitical dynamics. Given its central role in operations, technology is now a primary driver. When infrastructure becomes foundational, it inevitably becomes consequential.

The ICC episode illustrates this transition in a concrete way. A decision taken in one domain – legal and political – translated directly into consequences in another: access to digital services. This illustrates how interconnected legal, operational, and technological systems can interact under specific conditions. What had long been perceived as stable and continuously available proved to depend on provisions beyond the immediate control of the organisation using it. This raises an important question about dependency. What does access actually depend on?

The answer turns out to be layered. Access depends on systems, but also on jurisdictions. On contracts, but also on regulation. On architecture, but also on decisions made beyond the organisation itself. In a globally interconnected digital economy, no system stands alone. That interconnectedness has delivered enormous benefits. The rise of cloud platforms, AI services and global software ecosystems has enabled organisations to innovate faster, scale more efficiently, and operate across borders with unprecedented ease. Much of today's digital progress would simply not exist without this level of integration. Large technology providers – hyperscalers – are a central part of that reality. They have become foundational to how digital systems are built and operated. Their scale, capabilities and continuous innovation make them seemingly indispensable in practice. Often, they are not external to the system. They are part of its core. Which makes the issue more nuanced. Organisations almost always have to rely on these ecosystems in one way or another. The real challenge is deciding how to structure that relationship.

Over time, many organisations have optimised their technology landscape for speed, efficiency and convenience. Each decision made sense in isolation: adopt the most capable platform, integrate the most advanced service, rely on the most scalable infrastructure. Logical steps, taken one after another. But collectively, they form something else. A structure. A structure in which dependency is no longer designed, but accumulated.

The ICC case makes this visible. It shows how dependencies that are operationally efficient under normal conditions can become constraints when conditions change. Not because the technology is unreliable, but because it operates within a broader framework that can shift. This very realisation has led the ICC to replace its office platform with Open Desk, an open-source system provided by the German company ZenDis.[4] This is where the sovereignty discussion begins – not as a political stance, but as a practical necessity.

Digital sovereignty is often framed in terms of ownership or control: where technology is built, who provides it, which region governs it. But in practice, those dimensions only tell part of the story. What matters more is whether organisations retain the ability to make meaningful choices within that structure. Can they continue to operate if conditions change? Can they adapt when constraints emerge? Can they switch when switching becomes necessary? Sovereignty, in this sense, is not about independence. It is about optionality.

While this report is written from a European vantage point, shaped by its regulatory environment and its visible dependencies on global technology providers, the patterns described here are not uniquely European – they are systemic. Dependency, vendor lock-in, and exposure to external legal and commercial forces are structural features of a deeply interconnected digital economy, not regional anomalies. Even in the United States, where many of today's dominant platforms originate, organisations operate within concentrated ecosystems that create their own forms of reliance and constraint. The asymmetries may differ, but the underlying question is shared: how much control over critical technology is enough? Seen in this light, sovereignty is not a European exception or a political posture, but a broader reframing of risk, resilience, and strategic choice in a world where no actor is fully autonomous. The examples in this report serve exclusively to illustrate broader, systemic dynamics across the industry. They are not meant to critique individual organisations, providers, or jurisdictions.

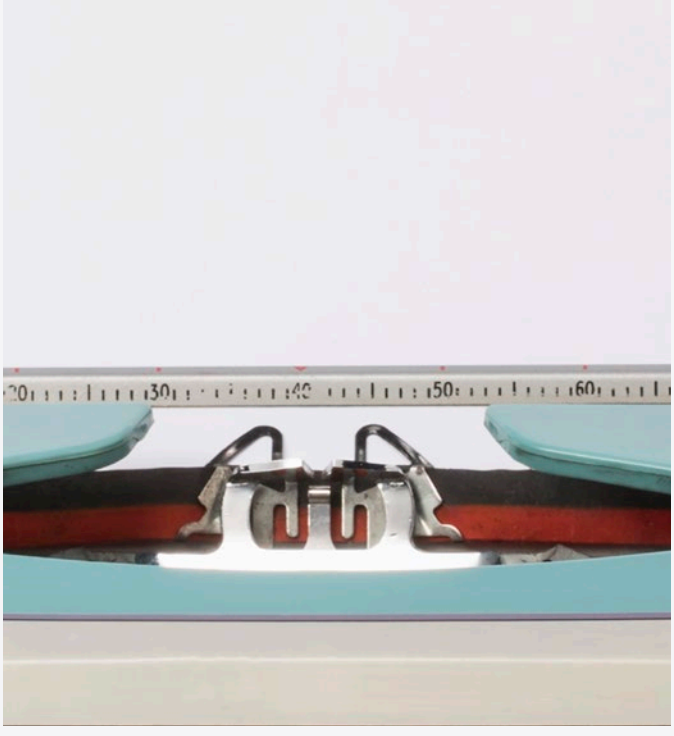
In a deeply interconnected system, full autonomy is neither realistic nor desirable. Every organisation depends on global supply chains – of hardware, software, data, energy and talent. The strength of the system lies precisely in that interdependence. But interdependence without clarity becomes something else. Not fragile, but conditional. Not unstable, but constrained. The challenge is to understand, rather than to eliminate dependency. To distinguish between what is convenient and what is critical. To recognise which systems can be replaced, which can be adapted, and which require stronger safeguards. Because not all technology carries the same weight. Some systems are interchangeable. Others are important. And a small number are foundational to continuity itself.

There is also a less visible dimension. Technology is not always neutral in practice. Norms and values are embedded in software, interfaces, algorithms, and AI systems, often in subtle but consequential ways.

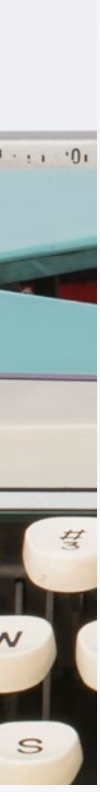
[4] Kerkmann, C. (2025, October). Strafgerichtshof ersetzt Microsoft durch deutsche Lösung. *Handelsblatt*. https://www.handelsblatt.com/technik/it-internet/software-strafgerichtshof-ersetzt-microsoft-durch-deutsche-loesung/100166382.html

As digital systems increasingly shape communication, decision-making, and even influence meaning, identity and sense-making, sovereignty also concerns the ability to remain attentive to the cultural assumptions built into the technologies on which we increasingly rely. Safeguarding digital autonomy is therefore a matter of infrastructure and regulation, but also of preserving cultural and institutional agency.

Recent developments can be interpreted as an inflection point. Current positions reflect years of accumulated interdependence, which means that any shift toward greater sovereignty will be gradual, selective and uneven. Historical examples suggest that reducing critical dependencies is possible through sustained coordination, long-term investment, and industrial collaboration. When Europe assessed its dependence on the American aircraft manufacturer Boeing to be too big, it contributed to the creation of Airbus. Such examples illustrate how strategic choices can reshape dependency structures over time.



That said, sovereignty should not be understood as a binary condition – sovereign versus non-sovereign – nor as a simple choice between European or foreign technology. In a deeply interconnected global economy, 100 percent sovereignty does not excist. Every organisation, including governments and strategic industries, operates within networks of dependency. The relevant question is therefore which dependencies are acceptable, under which conditions, and with which safeguards. Sovereignty is best understood as the outcome of a risk-based approach: balancing risk appetite, probability of disruption, regulatory exposure, mitigation measures, and credible exit options. This inevitably involves trade-offs between cost, speed of innovation, operational convenience, continuity, and long-term resilience.



Even in the case of Airbus, complete autonomy was never achieved. The company remains embedded in global supply chains. What such examples demonstrate is how coordinated long-term investment can reduce critical dependencies in strategically important layers.

This report approaches digital sovereignty from that perspective. It does not frame the issue as a competition between regions or providers. Nor does it assume that one model can substitute for another. It starts from the recognition that global ecosystems will remain essential, and that hyperscalers will continue to play a role within them. The question is how to participate while preserving room for manoeuvre.

To explore this, we introduce three recurring patterns through which access can become constrained: systems, markets and culture. Together, they describe how control in the digital age is distributed across multiple layers – technical, economic and conceptual. "Access Denied" is not an anomaly in this environment. It is a signal. A moment in which hidden dependencies become visible, and implicit assumptions are tested.

The organisations that navigate this successfully will be the ones that understand dependency, shape it, and where needed, redesign it. Because in the end, sovereignty in an interconnected world is about ensuring that when conditions change, the ability to act does not disappear with them.

Three gates of Access Denied

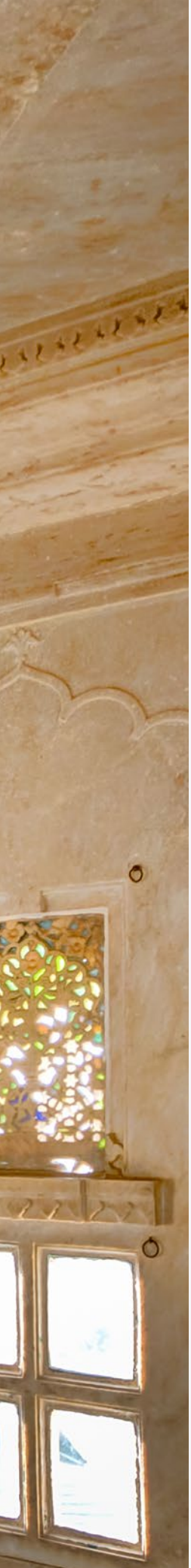
From this perspective, three variants of "Access Denied" can be distinguished – three ways in which dependencies may translate into constraints:

1. **Systems – the digital kill switch**
   Access to systems, data, and communication channels may be affected by legal, regulatory, or operational decisions within the jurisdictions in which service providers operate.
2. **Markets – the economic lever**
   Access to markets can be influenced by trade measures, regulatory requirements, or compliance conditions, which may affect organisations' ability to operate internationally.
3. **Culture – embedded norms, values and assumptions**
   Technology can carry implicit norms, values and design choices that influence how information is processed, decisions are made, and interactions take place.

Together, these layers illustrate how dependencies can manifest across infrastructure, economic relationships, and cultural influence. Based on this framework, this report explores the following questions:

1. How have these dynamics developed, and what is at stake?
2. What does the current landscape look like in terms of initiatives, approaches, and capabilities? What ideas, initiatives and companies exist to make Europe digitally sovereign?
3. How feasible are different paths forward, and what developments can be expected in the coming years?
4. What should the CIO's Sovereignty agenda look like?

Chapter 1
The golden cage



For more than a decade, Europe has expressed the ambition to strengthen its position in the digital domain.[5] Yet for many years, this ambition remained largely abstract for the average IT leader. That situation is now changing. Digital technologies have become deeply intertwined with economic competitiveness, scientific progress, and, increasingly, geopolitical dynamics. Concepts such as strategic autonomy, resilience, security, and democratic control are gaining prominence. But what do these terms mean in practice? And how should sovereignty be understood in a highly interconnected digital world?

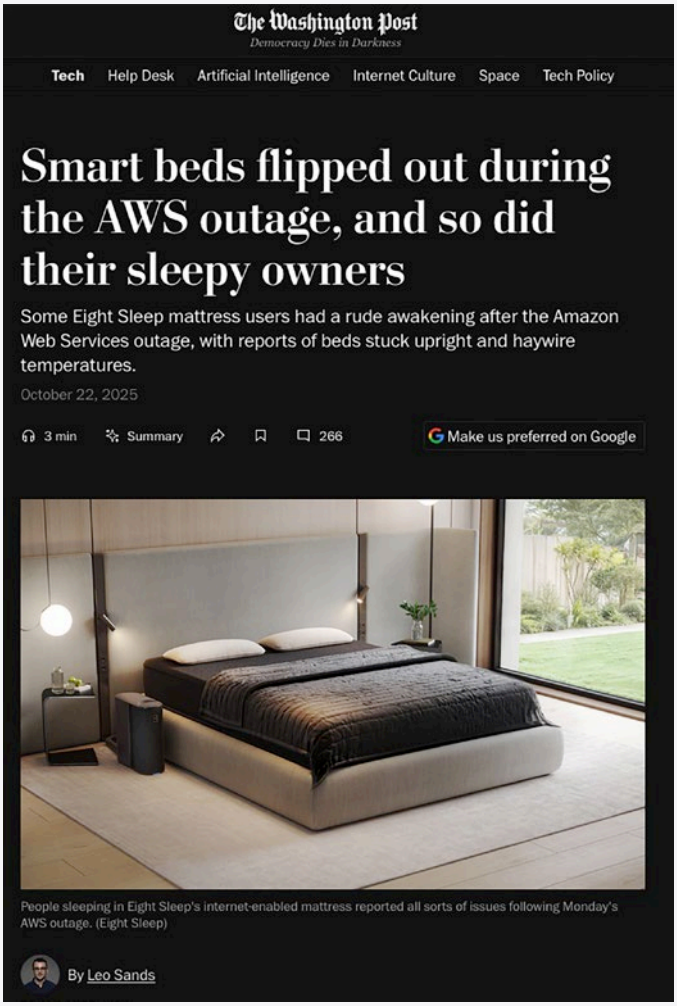
To explore these questions, it is useful to first examine how the current situation emerged.

Over the past four decades, a global digital ecosystem has taken shape, largely driven by technological breakthroughs originating outside Europe. From early operating systems in the 1980s, to the rise of the internet in the 1990s, to the mobile revolution and, more recently, the emergence of large-scale artificial intelligence platforms, many of the most widely adopted technologies have been developed and scaled by companies based primarily in the United States and China. These solutions often combined usability, scalability, and rapid innovation, leading to widespread global adoption, including across Europe.

What was widely perceived as technological progress and economic opportunity has also resulted in a high degree of integration with external digital infrastructures, creating a proverbial golden cage. Data flows, cloud services, and digital platforms have become deeply embedded in European economies and institutions, frequently operated by providers headquartered outside Europe. This has created a situation in which legal frameworks from multiple jurisdictions may apply simultaneously.

[5] Kenniscentrum Europa Decentraal. (n.d.). *Digitale Overheid.* https://europadecentraal.nl/onderwerp/digitale-overheid/

Legislation such as the USA PATRIOT Act and the CLOUD Act illustrates how national legal systems can extend beyond territorial borders in the context of digital services. Under certain conditions, these frameworks may enable authorities to request access to data managed by companies subject to their jurisdiction, even when that data is stored elsewhere. While such mechanisms are typically justified within their respective legal and security contexts, they also raise questions about how different jurisdictions interact in practice, particularly when data, infrastructure, and services span multiple regions.



The Washington Post
Democracy Dies in Darkness

Tech Help Desk Artificial Intelligence Internet Culture Space Tech Policy

Smart beds flipped out during the AWS outage, and so did their sleepy owners

Some Eight Sleep mattress users had a rude awakening after the Amazon Web Services outage, with reports of beds stuck upright and haywire temperatures.

October 22, 2025

3 min Summary 266 Make us preferred on Google

People sleeping in Eight Sleep's internet-enabled mattress reported all sorts of issues following Monday's AWS outage. (Eight Sleep)

By Leo Sands

Our dependence on Big Tech permeates every aspect of our lives. Owners of Eight Sleep smart mattresses experienced this firsthand when their beds turned scorching hot, lights and alarms went off, and the mattress got stuck in an upright position. All because Amazon Web Services was down.[6]

This has contributed to a broader discussion within legal and policy communities. When cross-border legal claims intersect with critical digital infrastructure, the distinction between commercial service provision, legal compliance, and strategic interests can become less clear-cut. Rather than representing a conflict in the traditional sense, these situations highlight the complexity of operating in a globally interconnected system, where multiple legal and regulatory regimes coexist and occasionally overlap.

From integration to dependency

The increasing reliance on globally provided digital services has brought significant benefits, including innovation, efficiency, and scalability. At the same time, it has introduced forms of dependency that are now receiving greater scrutiny. For many organisations, digital infrastructures have become so deeply embedded in operations that switching providers or redesigning systems would involve substantial economic and operational costs that could effectively proof prohibitive.

Recent developments have brought these dynamics into sharper focus. A number of high-profile incidents – ranging from access restrictions to digital services, to shifts in platform policies,[7] to changes in the availability of critical infrastructure[8] – have been widely discussed in policy and media circles. These events are interpreted in different ways, but collectively they have contributed to a growing awareness of how digital dependencies can intersect with legal, political, and operational considerations.

Importantly, such dynamics are not unique to any single country or region. As digital platforms scale globally, similar patterns of dependency and influence can emerge regardless of origin. Large technology ecosystems, by their nature, tend to concentrate capabilities and create forms of lock-in that are difficult to unwind.

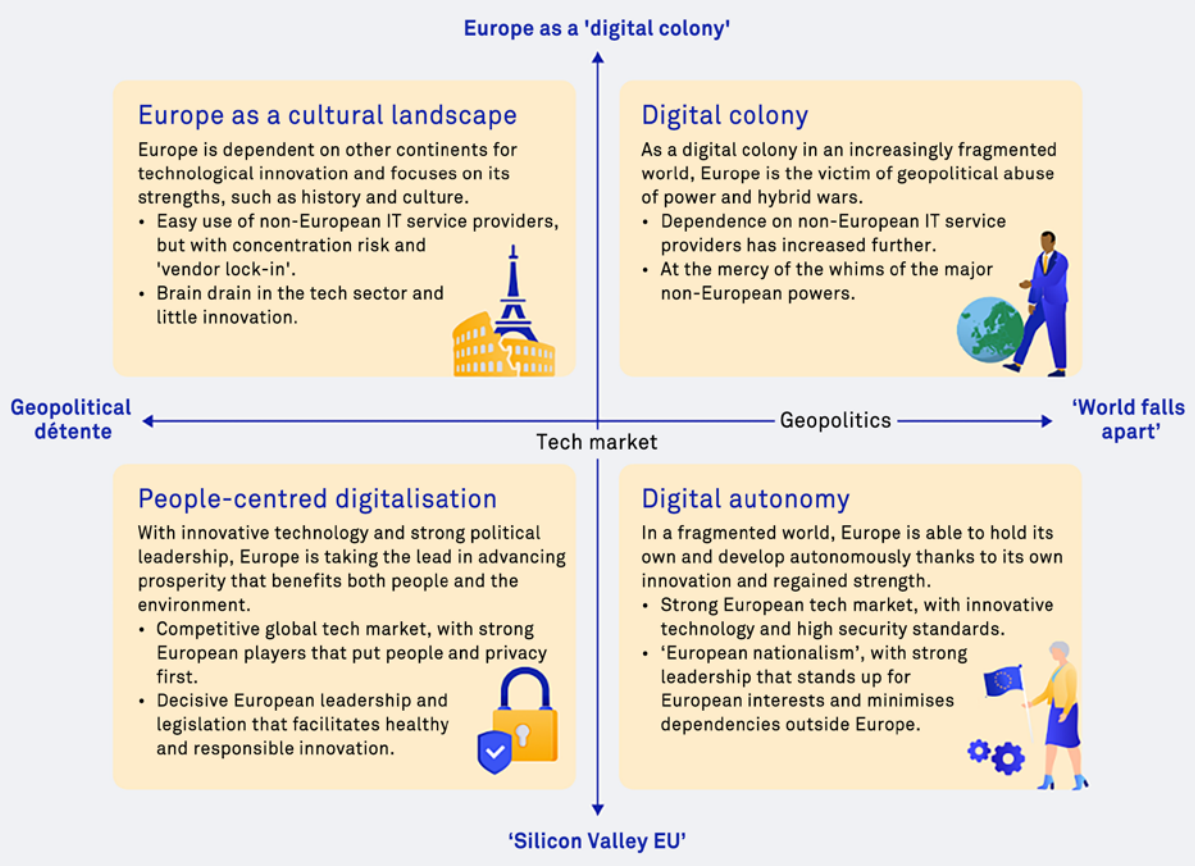
This broader concern is reflected across multiple sectors. In October 2025, for example, Dutch financial regulators, including De Nederlandsche Bank and Authority for the Financial Markets, highlighted the increasing reliance of financial institutions on a limited number of large technology providers.[9] Their analysis pointed to potential concentration risks and emphasized the importance of resilience, diversification, and contingency planning

[6] The Washington Post. (2025, October 22). *Smart beds flipped out during the AWS outage, and so did their sleepy owners*. https://www.washingtonpost.com/technology/2025/10/22/amazon-aws-outage-eight-sleep-mattress/

[7] Lekander, A. (2025, March 14). *Signal No Longer Cooperating with Ukraine to Tackle Russian Cyber Threats*. CyberInsider. https://cyberinsider.com/signal-no-longer-cooperating-with-ukraine-to-tackle-russian-cyber-threats/

[8] Denisova, K. (2025, March 9). Ukrainian front line 'would collapse' if Starlink is turned off, Musk claims. *The Kyiv Independent*. https://kyivindependent.com/ukrainian-front-line-would-collapse-if-starlink-is-turned-off-musk-claims/

[9] De Nederlandsche Bank. (2025, October 20). *AFM en DNB waarschuwen voor systeemrisico's financiële sector door digitale afhankelijkheid*. https://www.dnb.nl/algemeen-nieuws/persbericht-2025/afm-en-dnb-waarschuwen-voor-systeemrisico-s-financiele-sector-door-digitale-afhankelijkheid/



DNB warns against excessive digital dependence in the financial sector. It has developed four future scenarios, divided along the axes of "Geopolitics" and "Techmarket". They use strong language to describe potential long-term dependency risks, highlighting concerns about structural reliance on external digital ecosystems. To change course, public and private parties will have to work more closely together.

The report does not frame these dependencies in geopolitical terms alone, but rather as systemic risks inherent in highly concentrated digital ecosystems. It suggests that organisations and regulators should consider how to maintain operational continuity under a range of scenarios, including those influenced by legal, regulatory, or market developments in other jurisdictions.

Similar patterns can be observed in the industrial domain. Dependencies on specialized software, supply chains, and advanced technologies – such as electronic design automation tools – illustrate how deeply integrated global production systems have become.[10] Changes in export controls or regulatory frameworks in one region can have immediate and sometimes unexpected effects elsewhere, underscoring the interconnected nature of modern industry.

[10] Bloomberg. (2025, July 3). *Chip Design Software Makers Win US Reprieve in China Trade Deal*. https://www.bloomberg.com/news/articles/2025-07-03/siemens-says-us-has-rescinded-chip-software-curbs-on-china

[11] Donald J. Trump (2nd Term). (2025, February 21). *Memorandum on Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties*. The American Presidency Project. https://www.presidency.ucsb.edu/documents/memorandum-defending-american-companies-and-innovators-from-overseas-extortion-and-unfair

Shifting leverage at the negotiating table

As digital technologies become more central to economic activity, they are increasingly intersecting with broader policy and trade discussions. This is visible, for example, in policy statements such as the memorandum "*Defending American Companies and Innovators from Overseas Extortion and Unfair Fines and Penalties*", issued by Donald Trump.[11]

"As the President of the United States, I will stand up to Countries that attack our incredible American Tech Companies. […] unless these discriminatory actions are removed, I, as President of the United States, will impose substantial additional Tariffs on that Country's Exports to the U.S.A., and institute Export restrictions on our Highly Protected Technology and Chips."

– Donald Trump

The language of the memorandum reflects a perspective in which regulatory measures affecting technology companies are linked to wider economic and trade considerations, illustrating how digital policy and trade policy can become interconnected in different jurisdictions. It signals that taxes, regulatory measures and legislative frameworks affecting major American technology companies may become part of broader trade negotiations, and also indicates that where such measures are perceived as discriminatory, countermeasures– including tariffs and export restrictions – may follow.

For Europe, this illustrates how closely digital policy, industrial competitiveness and geopolitical bargaining have become intertwined. Only weeks earlier, a trade agreement had created expectations of relative stability. Ursula von der Leyen acknowledged at the time that the agreement was imperfect, yet emphasised that Europe had maintained its regulatory principles. Although digital regulation had initially remained outside tariff negotiations, it quickly returned to the centre of political discussion.

"Our rules remain intact […] We are the ones who decide how best to safeguard food safety, protect European citizens online, and ensure their health and safety."

– Ursula von der Leyen

These parallel positions illustrate how digital policy is becoming part of a broader landscape in which regulation, trade, and industrial strategy are increasingly interconnected. Instruments such as the Digital Services Act, the Digital Markets Act, and the AI Act are designed to address specific challenges related to platform responsibility, market competition, and emerging technologies. At the same time, their implementation takes place within a global context in which multiple regulatory approaches coexist.

The key observation is not that regulatory sovereignty is diminished, but that it is exercised within a more complex environment. Digital infrastructures and platforms operate across borders, and this influences the conditions under which regulatory frameworks are developed and enforced. This complexity is most clearly visible in the emergence of landmark European regulations such as the DSA, DMA, and AI Act.

Digital Services Act (DSA): responsibility for content

Key point: Platforms such as Meta, X, Google and TikTok must monitor illegal and harmful content much more strictly.

The following applies to Big Tech:

- They are obliged to remove illegal content (hate speech, disinformation, counterfeiting) more quickly.
- They must provide transparency about their algorithms (recommendation systems) and offer users options to view algorithm-free feeds.
- Access for regulators and researchers: Big Tech must open up data, radically breaking with their "black box" approach.

Digital Markets Act (DMA): power of the gatekeepers

Key point: Large platforms that act as gatekeepers, such as Google, Apple, Amazon, Meta, Microsoft and TikTok, may no longer abuse their market power.

The following applies to Big Tech:

- Prohibition of self-preference: Google may no longer give priority to its own services (Maps, Shopping, YouTube) in search results.
- Interoperability: WhatsApp, for example, must become accessible to other messaging services.
- Prohibition on data linking: Meta may not simply combine data from Facebook, Instagram and WhatsApp for advertising purposes without consent.

Artificial Intelligence Act (AI Act): limits on risky AI

Key points: First globally binding framework for artificial intelligence, with an emphasis on risk mitigation. For Big Tech, the following applies:

- Ban on certain AI applications (e.g. similar to China's social scoring, manipulative AI that influences children, or real-time biometric surveillance in public spaces).
- Strict obligations for "high-risk AI" (e.g. in HR, the judiciary, healthcare and infrastructure): transparency, human control and documentation.
- Generative AI models such as GPT-5, Gemini and Claude are subject to additional rules: transparency about data training, protection against harmful outputs and mandatory labelling of AI content.

Several countries have also introduced taxes on Big Tech companies – the so-called Digital Services Tax (DST) – which has now become another bargaining chip in the negotiations. Under US pressure, Canada abolished its DST in June 2025. In the United Kingdom the tax currently raises around £800 million annually from Big Tech companies, yet even there, it was scaled back following the threat of sweeping US import tariffs that would have severely harmed the British automotive industry.[12]

[12] Crearer, P., Stewart, H. & Partington, R. (2025, April 2). Starmer offers big US tech firms tax cuts in return for lower Trump tariffs. *The Guardian*. https://www.theguardian.com/us-news/2025/apr/01/starmer-offered-big-us-tech-firms-tax-cuts-in-return-for-lower-trump-tariffs

Getting used to the new face of Big Tech: Full Stack Integration

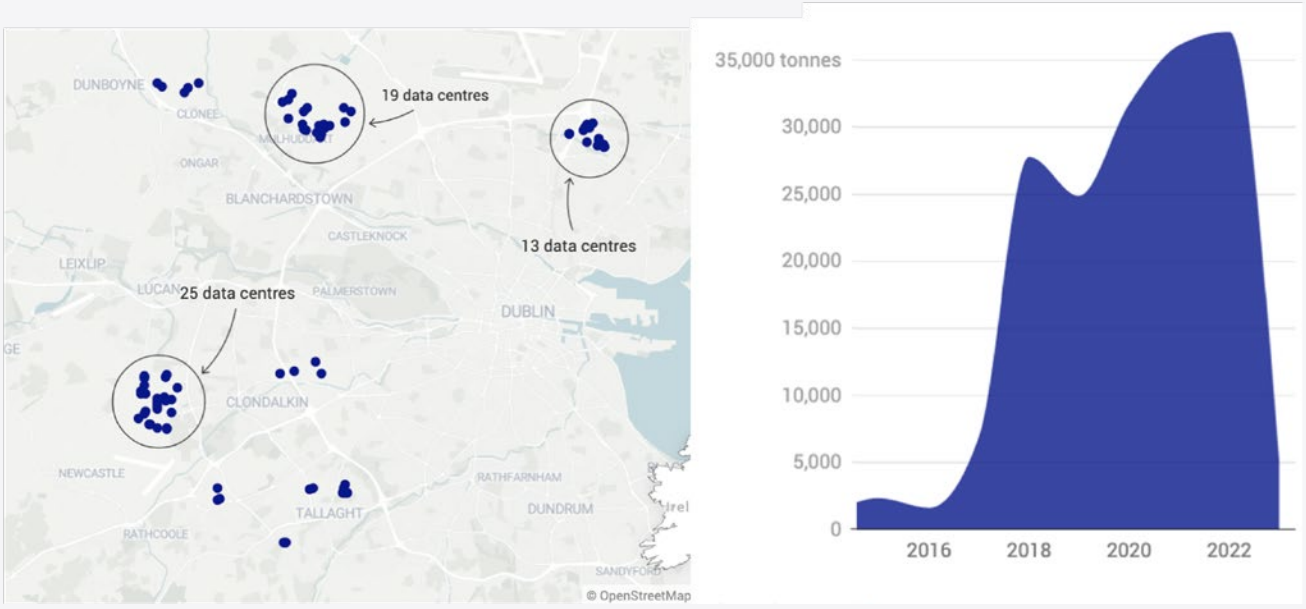
Alongside these developments, large technology providers continue to expand their capabilities across multiple layers of the digital stack. What is emerging is a form of vertical integration in which infrastructure, platforms, data, and applications become increasingly interconnected within the same ecosystem.

This trend is particularly visible in the field of artificial intelligence. As noted in publications such as *The Atlantic*,[13] concerns have been raised about potential forms of technological lock-in associated with proprietary AI platforms, such as Open-AI. Organisations that build workflows, data pipelines, and applications around specific models or ecosystems may find it challenging to switch providers without significant effort. OpenAI, like many large-scale platform providers, is evolving toward a more tightly integrated ecosystem in which users, data and tools become tightly coupled to its infrastructure. Code and workflows are optimised for proprietary AI models and aligned with vendor-specific storage formats. API-dependencies and *prompt tuning* pull organisations deeper into a single supplier's value chain.

At the same time, these developments are accompanied by rapid innovation and substantial investment, which continue to drive technological progress. The resulting landscape is therefore characterized by both opportunity and concentration: powerful new capabilities on the one hand, and increasing integration on the other.

In the UK, concerns about AI lock-in have intensified since the government signed an agreement with OpenAI in the summer of 2025.[14] The deal provides for the deployment of ChatGPT on so-called sovereign servers, powered by NVIDIA-supplied GPUs, under the banner "Stargate UK" – a name deliberately echoing the earlier US arrangements between government and Big Tech. UKAI, a coalition of domestic AI companies, calls it short-sighted.[15] Cultural figures have also voiced alarm: Elton John, for example, has warned that OpenAI poses a growing threat to the British creative industries, where copyright protection is already under strain. As part of the deal, OpenAI will increase its presence in the UK and support various government chatbots. One detail is particularly revealing: the Secretary of State for Technology who signed the deal is an enthousiastic user of ChatGPT himself, reportedly relying on it for advice, including on how the UK should maintain its leadership in the global AI race.[16]

According to investigative journalist Karen Hao, OpenAI and other Big Tech AI companies should be considered empires.



Left: *The Journal* found 89 operational data centres in Ireland. The majority are located in Dublin.

Right: CO_2 emissions measured by backup and emergency generators at Irish data centres. The rising electricity demand of these data centres is at odds with Ireland's climate goals.[17]

Some commentators, such as Karen Hao, interpret these developments through a historic lens, suggesting parallels with earlier forms of economic and technological concentration. She argues that the UK is effectively partnering with an empire. In her book *Empire of AI*, the investigative journalist traces how OpenAI transformed from an idealistic, mission-driven nonprofit into a commercial behemoth valued at more than $800 billion. Drawing on more than 300 interviews with some 260 individuals, Hao dissects the company with forensic precision. She contends that the anology with historical colonial empires can be interpreted as structural: arguing that AI companies, like Europe's former imperial powers, appropriate resources that are not theirs. They rely extensively on publicly available human knowledge and creativity embedded in online content. This perspective raises questions about how value, ownership, and governance are defined in large-scale AI systems. The prevailing narrative, she argues, is a familiar imperial one: the 'good' empire must expand and extract in order to defeat the 'bad' empire. In reality, Hao concludes, no nation today wields more concentrated power than these companies.

These differing interpretations highlight that the current transformation is still unfolding. There is no single consensus on how these dynamics will evolve, but there is broad agreement that scale, integration, and resource access – ranging from data to energy – are becoming increasingly important factors.

[13] Wong, M. (2025, April 22). The Great AI Lock-In Has Begun. *The Atlantic*. https://www.theatlantic.com/technology/archive/2025/04/openai-lock-in-profit/682538/

[14] OpenAI. (2025, July 21). *OpenAI and UK government announce strategic partnership to realise AI-supported growth*. https://openai.com/nl-NL/global-affairs/openai-and-uk-government-partnership/

[15] Courea, E. & Stacey, K. (2025, August 23). Deal to get ChatGPT Plus for whole of UK discussed by Open AI boss and minister. *The Guardian*. https://www.theguardian.com/politics/2025/aug/23/uk-minister-peter-kyle-chatgpt-plus-openai-sam-altman

[16] Stacey, K. (2025, March 13). Technology secretary Peter Kyle asks ChatGPT for science and media advice. *The Guardian*. https://www.theguardian.com/politics/2025/mar/13/technlogy-secretary-peter-kyle-asks-chatgpt-for-science-and-media-advice

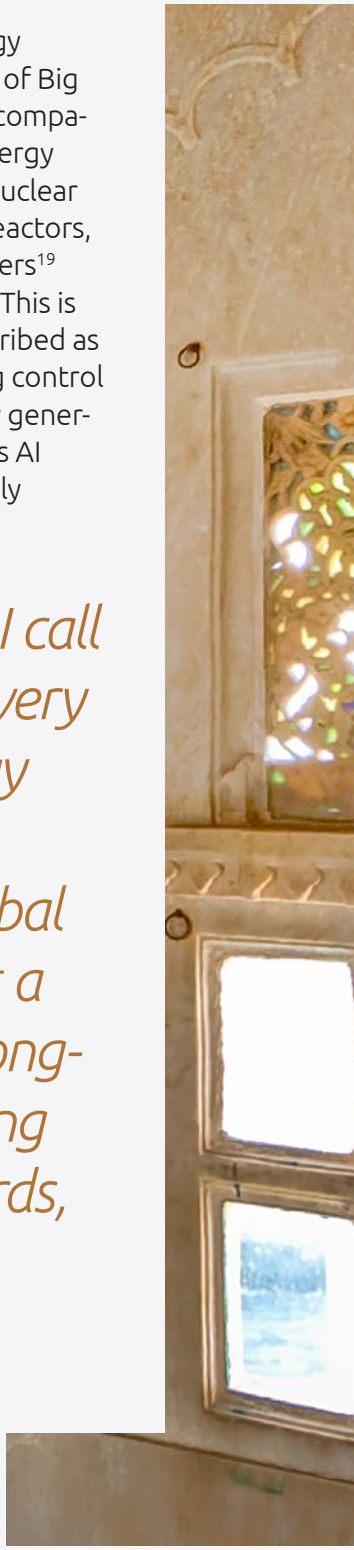
[17] O'Carroll, C. (2024, November 28). Ireland's data centres turning to fossil fuels after maxing out country's electricity grid. *The Journal*. https://www.thejournal.ie/investigates-data-centres-6554698-Nov2024/

The growing role of energy infrastructure provides a concrete example. Data centres, particularly those supporting AI workloads, are consuming increasing amounts of electricity. In countries such as Ireland, data centre demand has become a significant component of national energy usage, prompting discussions about infrastructure planning, sustainability, and long-term capacity.[18] This illustrates how digital technologies are no longer confined to the virtual domain, but are increasingly linked to physical resources such as energy, land, and materials.

The explosive growth in data centre energy consumption is reshaping the very nature of Big Tech. To sustain their AI ambitions, these companies have become serious actors in the energy market. They are securing capacity from nuclear power plants, reviving decommissioned reactors, forming new ventures with energy providers[19] and even building their own gas turbines. This is the emergence of what is now being described as "full-stack" Big Tech: Digital giants seeking control across the entire value chain, from energy generation to foundational language models. As AI expert and author Nina Schick puts it, "Only full-stack control wins the AI war."[20]

"Power in AI comes only through what I call Full Stack Control: sovereignty across every layer of the AI value chain – from energy and raw materials, through chips and data, to models, infrastructure, and global deployment. Full Stack Control isn't just a tech strategy – it's the foundation for long-term geopolitical advantage, determining which nations will set the rules, standards, and terms of global influence in the decades to come."

– Nina Schick



Conclusion

Taken together, these developments point to a shift in how digital technologies are positioned within the broader economy. What was once primarily a matter of software and services is now closely connected to infrastructure, supply chains, and industrial capacity.

For Europe, this raises strategic questions rather than binary choices. How to engage in global technology ecosystems in a way that balances innovation, resilience, and control? This involves considering a range of options, from diversification of suppliers to investment in domestic capabilities, and from regulatory frameworks to international cooperation.

Regulation alone is unlikely to address all aspects of this challenge. While instruments such as the Digital Markets Act and the Digital Services Act play an important role in shaping market behaviour and protecting public interests, they operate within a broader system in which technological capabilities, infrastructure, and economic scale are also determining factors.

The central insight is that digital sovereignty, in practice, is about maintaining sufficient strategic optionality. In an interconnected world, this means understanding dependencies, managing risks, and ensuring that critical capabilities remain accessible under a range of conditions.

Rather than framing the issue as a confrontation between regions, it is more accurately understood as a structural characteristic of the global digital economy – one that requires careful navigation, informed decision-making, and a long-term perspective. Beneath the dilemma between dependencies and convenience lies a deeper miscalculation. As long as Europe treats AI primarily as a matter of market regulation and compliance, it overlooks where real power resides; with those who control data, hardware and energy infrastructure.

[18] Moss, S. (2024, July 23). *Irish data centres used more than 21 per cent of nation's total metered electricity.* DCD. https://www.datacenterdynamics.com/en/news/irish-data-centers-used-more-than-21-percent-of-nations-total-metered-electricity/

[19] Nuclear Business Platform. (2023, May). *Why Tech Giants Are Investing Billions in Nuclear Power Over Renewables?* https://www.nuclearbusiness-platform.com/media/insights/tech-giants-are-investing-billions-in-nuclear

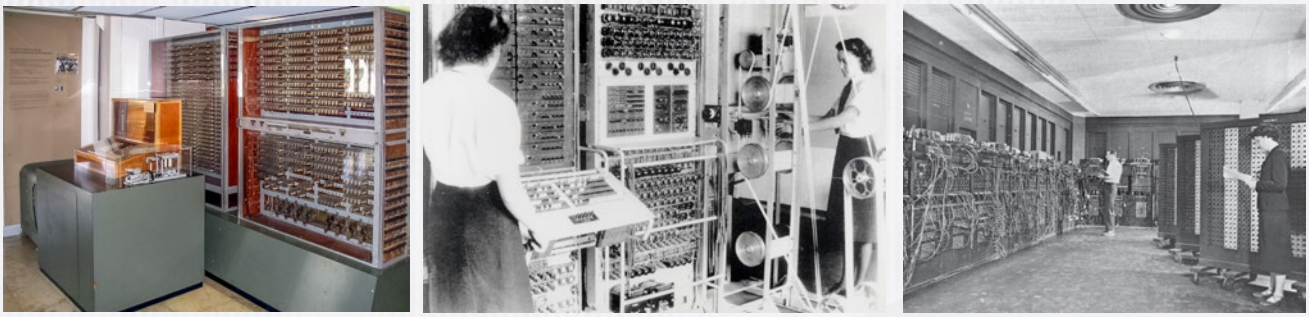
[20] Schick, N. (2025, May 23). *Only Full Stack Control Wins the 'AI War'.* https://ninaschick.substack.com/p/only-full-stack-control-wins-the-ai-war/

Chapter 2
What is sovereignty?

The concept of sovereignty has deep historical roots. It is often associated with the Peace of Westphalia of 1648, which helped – after thirty years of war – establish a lasting principle of European political order: that states exercise authority within recognised borders and without external interference. What made the agreement historic was not merely the end of the violence, but the principles on which peace was forged. The Pope could no longer dictate worldly affairs. No emperor could impose his will on other monarchs. Each state was granted the right to determine its own laws, religion and form of government within its own borders. Sovereignty was defined – not as an abstract ideal, but as a mutual recognition that authority exists only when others accept its limits.

So sovereignty essentialy concerns the ability to make and enforce decisions within a defined domain without being overruled by an external authority. Traditionally, this domain was territorial. Today, however, questions of sovereignty increasingly extend beyond physical borders into the digital realm. In modern economies, control over data, compute capacity, cloud infrastructure, software platforms, semiconductors, and AI models increasingly shapes economic resilience, institutional autonomy, and strategic room for manoeuvre.

This does not mean that digital systems replace territorial sovereignty, but it does mean that sovereignty now has an additional dimension. Where earlier eras focused on land, military force, and political jurisdiction, the present era also requires attention to control over the infrastructures that enable communication, decision-making, public services, and scientific research.



From left to right: the Z3, the Colossus and the ENIAC. These first-generation computers were all national strategic assets intended for sovereign purposes.

Early computing as strategic infrastructure

The strategic importance of computing is not new. In the first half of the twentieth century, major advances in computing emerged in close connection with state priorities, particularly during wartime. In Germany, Konrad Zuse built the Z3 in 1941, widely regarded as one of the first programmable digital computers. In the United Kingdom, Colossus was developed under strict secrecy to support wartime codebreaking. In the United States, ENIAC followed in 1945 and was initially used for military calculations before becoming part of broader scientific and defence-related research.

These early machines were treated as critical assets tied to national capability, military effectiveness, and scientific capacity. After the Second World War, advanced computing became increasingly concentrated in the United States, where sustained investment by government, universities, and industry helped lay the foundations for what would later become the modern digital technology sector. European countries, rebuilding after the war and operating within more fragmented industrial structures, developed important capabilities of their own, but often at a different scale.

This historical pattern helps explain part of today's landscape. The concentration of cloud computing, advanced semiconductors, large-scale AI infrastructure, and digital platforms in a relatively small number of non-European companies did not emerge overnight. It reflects a longer trajectory in which computing capacity, capital, and platform scale became concentrated outside Europe.

The underlying question, however, remains similar across time: which capabilities are sufficiently critical that they should remain subject to meaningful public, regional, or organisational control?

Scientific data and strategic dependence

In recent years, sovereignty concerns have also become visible in the management of scientific data. Several European institutions have taken steps to archive, mirror, or secure continued access to critical datasets that are hosted or governed outside Europe. These measures are generally precautionary in nature and reflect a growing awareness that scientific infrastructure, like digital infrastructure more broadly, can become strategically significant.

In the Netherlands, organisations such as SURF (cooperative organisation that develops, implements and maintains the national research and education network) and KNMI (Royal Netherlands Meteorological Institute) have expressed concern about continued access to important climate and atmospheric datasets historically managed by institutions in the United States.[21] Similar considerations have emerged elsewhere in Europe. Denmark has taken steps to download historical climate data from NOAA (National Oceanic and Atmospheric Administration). Norway has funded backup measures for certain critical datasets. Germany has reviewed dependencies on external scientific data sources. At the European level, initiatives are underway to strengthen data-sharing and observation capabilities in areas such as marine and climate research.

These developments suggest that access to scientific data is no longer viewed purely as a matter of research efficiency. It is increasingly regarded as part of a broader question of continuity, resilience, and strategic autonomy. Scientific datasets often underpin much more than academic work. They also support insurance modelling, infrastructure planning, climate adaptation, energy investments, emergency preparedness, and public policy.

This is particularly clear in the case of NOAA, which has for decades played a central role in global climate and atmospheric data infrastructure. Its measurement series and observational systems support not only science but also a wide range of operational and economic functions. When data infrastructures of this kind are concentrated in one country or under one institutional framework, changes in funding priorities, policy direction, or governance can have international consequences.

[21] Schaap, S. (2025, April 22). *Wetenschappers halen stilletjes al onderzoeksdata weg uit VS om toegang te houden.* NOS Nieuws. https://nos.nl/collectie/13871/artikel/2564520-wetenschappers-halen-stilletjes-al-onderzoeksdata-weg-uit-vs-om-toegang-te-houden

Sovereignty beyond territory

These developments raise a broader conceptual question: what does sovereignty mean in a digitally interconnected world?

In classical political theory, sovereignty referred to the highest authority within a defined territory. Thinkers such as the sixteenth century, French jurist Jean Bodin described it as the ultimate and enduring power of the state: the ultimate decision-making authority, neither delegated nor shared with any external power. That definition remains important, but in practice it no longer captures the full picture. In highly networked societies, formal legal authority may coexist with operational dependence on external infrastructures, platforms, and providers.

This is why more recent interpretations of sovereignty increasingly focus not only on legal authority, but also on effective control. In this view, sovereignty is the practical ability to act, govern, adapt, and intervene when systems are under pressure. Applied to the digital domain, this means asking whether a state, organisation, or institution can understand, audit, influence, and, where necessary, modify the technologies on which it depends.

To make this more concrete, commentators such as Dutch technology expert Bert Hubert,[22] former AIVD (Dutch general intelligence and security service) employee, have argued that digital sovereignty should be understood in operational terms. His proposal for a sovereign Dutch cloud, under the label "Cloud Kootwijk," draws a historical analogy with the early twentieth-century communications infrastructure at Radio Kootwijk, which gave the Netherlands direct control over long-distance communications with the Dutch East Indies in a strategically important period.

Whether or not one agrees with the analogy, the underlying point is clear: sovereignty in the digital domain is not primarily symbolic. It depends on whether meaningful control exists in practice. That can be assessed through a few basic questions:

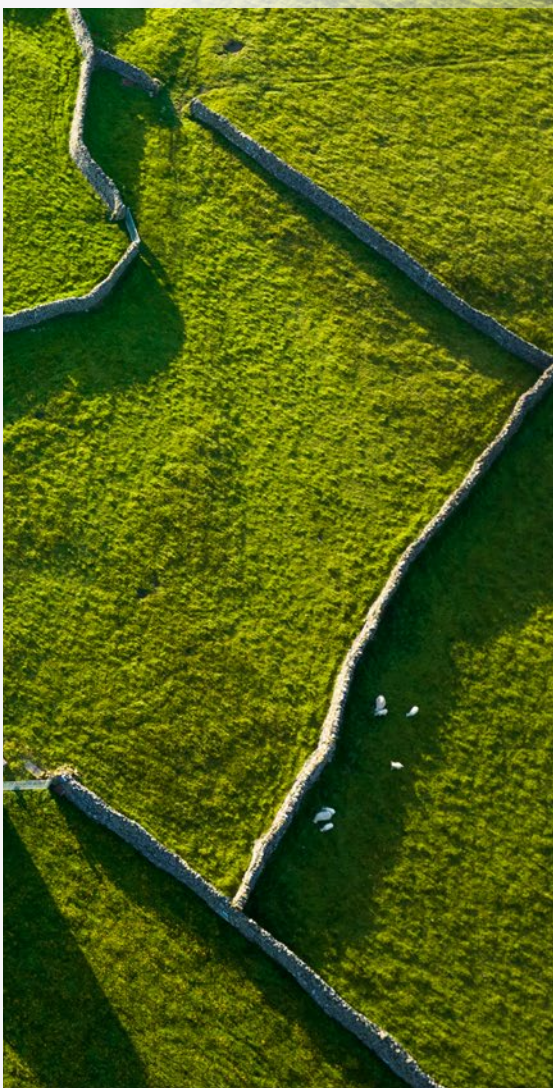
1. **Confidentiality**: Do only authorized parties have access to the data?
2. **Availability**: Can access to systems or services be interrupted by an external decision beyond local control?
3. **Control**: If something goes wrong, is there sufficient technical, operational, or legal capacity to intervene?

[22] Hubert, B. (2025, June 20). *Is dit een soevereine cloud?* berthub.eu. https://berthub.eu/articles/posts/en-is-dit-dan-de-oplossing/

Seen in this light, digital sovereignty can be defined as follows:

Digital sovereignty is the capacity of a state, organisation, or individual to exercise effective control over digital infrastructure, data, software, and technological dependencies within the limits of a globally interconnected system.

This definition deliberately avoids the idea of absolute independence. Crucially, this “capacity” is not purely technical. As with traditional sovereignty, it exists only insofar as it is recognised and upheld by others. That recognition operates at multiple levels: from respect for territorial jurisdiction, to the legal and operational boundaries within which foreign technology providers are permitted to operate, and the ability to set, negotiate, and enforce the conditions under which digital power is exercised.



Why complete sovereignty is unrealistic

Once defined this way, it also becomes clear that complete digital sovereignty is neither realistic nor, in many cases, desirable. Modern technology systems depend on deeply international supply chains. Rare earth materials, advanced semiconductors, specialized manufacturing equipment, software platforms, cloud infrastructure, and network components are all distributed across multiple countries and sectors. No major economy operates entirely outside these interdependencies.

Recent developments have made this especially visible. Restrictions on the export of rare earth materials,[23] for example, have shown how dependent many industries remain on supply chains concentrated in a small number of countries.[24] Semiconductor-related disruptions have similarly illustrated how events in one jurisdiction can affect manufacturing capacity elsewhere. These patterns are not exceptional. They are characteristic of the global technology economy.

The cloud market provides another clear example. Europe's spending on public cloud services continues to rise rapidly (growing to €285 billion by 2027), while a substantial share of this market is served by a small number of large non-European providers. European cloud providers remain active, but their aggregate market share is smaller and, in many segments, under pressure.[25] This does not in itself imply failure. It does, however, highlight the degree to which critical digital functions are embedded in ecosystems headquartered elsewhere.

The same logic applies in the other direction. The United States and China also depend on external capabilities in certain areas. Advanced semiconductor production, for example, remains highly dependent on equipment supplied by ASML in the Netherlands.

[23] European Commission. (n.d.). *Critical raw materials*. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en

[24] Rutten, R. & Van Lonkhuyzen, L. (2025, October 21). Europa is al jaren afhankelijk van Chinese zeldzame aardmetalen, en incasseert nu de klap. *NRC*. https://www.nrc.nl/nieuws/2025/10/21/europa-is-al-jaren-afhankelijk-van-chinese-zeldzame-aardmetalen-en-incasseert-nu-de-klap-a4910277

[25] Bria, F., Timmers, P. & Genone, F. (2025). *EuroStack – A European Alternative for Digital Sovereignty*. Bertelsmann Stiftung. https://assets.filedock.xyz/public/EuroStack_2025.pdf

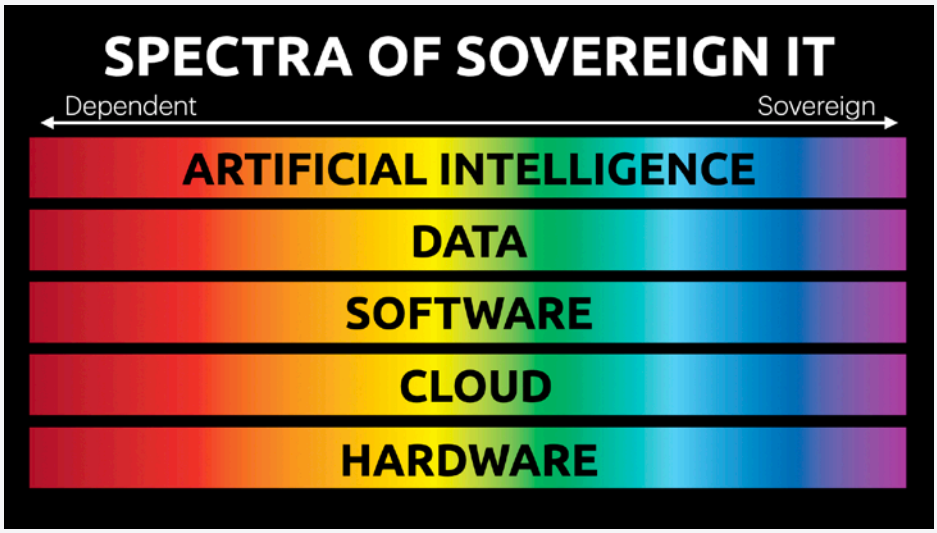
Sovereignty as a spectrum

Because complete control is unattainable, sovereignty is better understood as a matter of degree. States, sectors, and organisations can be more or less sovereign depending on which layers of the technology stack they control and which they rely on others to provide.

This layered view is useful. At the level of raw materials, Europe remains highly dependent on external suppliers. In specialized hardware, Europe has distinctive strengths, particularly in semiconductor equipment. In software, cloud, and workplace infrastructure, dependence is often greater, although this varies by use case and sector. At the organisational level, some public institutions have shown that meaningful increases in sovereignty are possible, especially when they deliberately choose open-source software or alternative digital architectures for specific functions.

Examples such as Schleswig-Holstein's migration away from Microsoft products, the long-term use of Linux by the French gendarmerie, and efforts by other governments to maintain greater control over operating systems and critical software environments suggest that selective sovereignty can be feasible. These examples do not demonstrate that full independence is possible. They do show that targeted reductions in dependency may be both technically and economically viable when applied to critical layers.

This is why sovereignty should be treated as a spectrum rather than a binary condition. The key question is not whether an organisation is sovereign in the abstract, but where greater control is necessary and where dependency is acceptable.



Because there are always dependencies in practice, we speak of spectra of sovereign IT.

Spectrum, scope and strategy

A practical approach to digital sovereignty therefore requires three questions.

The first concerns **spectrum**: how much control is needed at each layer of the IT stack? Not every layer has the same strategic importance, and not every organisation requires the same level of autonomy.

The second concerns **scope**: which systems, datasets, or processes actually require higher levels of sovereignty? A hospital may reach different conclusions from a retailer. Even within one organisation, certain applications may be non-critical, while others involve sensitive personal data, operational continuity, or public safety.

The third concerns **strategy**: what is driving the sovereignty requirement? In some cases, regulation is the main factor. In others, it may be resilience, continuity, security, cost, ethics, or institutional trust.

This framework helps move the discussion away from abstract slogans and toward proportional decision-making. In practice, digital sovereignty is often a form of risk management. The more critical a function is, and the greater the impact of disruption or loss of control, the stronger the case for retaining or building additional control, even if it seems more expensive or less efficient in the short term.


Access Denied

Regulation and operational responsibility

In Europe, this discussion is increasingly shaped by regulation. Frameworks such as NIS2 and the GDPR do not create sovereignty on their own, but they do make questions of control, accountability, and dependency more explicit.

The NIS2 Directive (Network and Information Security 2), which all Member States of the European Union are supposed to implement by 2024/2025, is designed to improve the resilience of organisations that provide essential or important services. It requires stronger governance, better risk management, greater visibility into supply chains, and clearer accountability at senior leadership level. One consequence is that organisations can no longer treat external providers as black boxes. They are expected to understand, monitor, and manage the dependencies on which their critical operations rely, which has a direct and profound impact on digital sovereignty

NIS2 operationalises sovereignty by imposing three concrete obligations: maintaining effective control over critical systems (duty of care), understanding and managing dependencies accross the supply chain (supplier responsibility), and participating in a coordinated European security framework through supervision and cooperation.

Crucially, NIS2 extends beyond an organisation's internal IT. It requires visibility into, and accountability for, the entire digital supply chain. This includes imposing contractual and security requirements on external providers such as cloud platforms, data centres, and software vendors. By making these dependencies explicit, NIS2 enables organisations to reassess their reliance on all technology providers to impose stricter conditions.

The GDPR (General Data Protection Regulation) addresses a related issue from the perspective of data governance. It strengthens the rights of individuals in relation to personal data and imposes strict conditions on how such data may be collected, processed, transferred, and stored. A central mechanism for achieving this is data minimisation combined with clearly defined ownership rights. Citizens retain enforceable control through rights such as access, rectification and erasure. This fundamentally alters the balance of power between individuals and organisations. A second pillar of the GDPR concerns localisation and international data transfers. Personal data relating to EU citizens cannot be freely exported outside the EU without adequate safeguards, forcing organisations to critically assess where and how data is processed and stored. Finally, the GDPR is backed by robust and harmonised European enforcement. Each Member State operates its own supervisory authority – such as the Dutch Data Protection Authority – but all act within a single, unified legal framework. Penalties of up to €20 million or 4 percent of global annual turnover ensure that even the largest multinational companies must comply.

This has implications for sovereignty because it requires organisations to think carefully about where data resides, under which legal regime it is processed, and how it can be protected against misuse or unauthorized access.

Again, the key point is not that regulation eliminates dependence. Rather, it changes the conditions under which dependence is acceptable.

Competing models of digital governance

The sovereignty debate also needs to be understood in an international context. Different regions have developed different approaches to digital governance, reflecting different priorities, institutional traditions, and political economies.

The European Policy Centre (EPC), a Brussels-based, non-profit think tank focused on European Union affairs, distinguishes between three broad models[26] of digital governance that coexist uneasily and, at times, stand in direct opposition to one another:

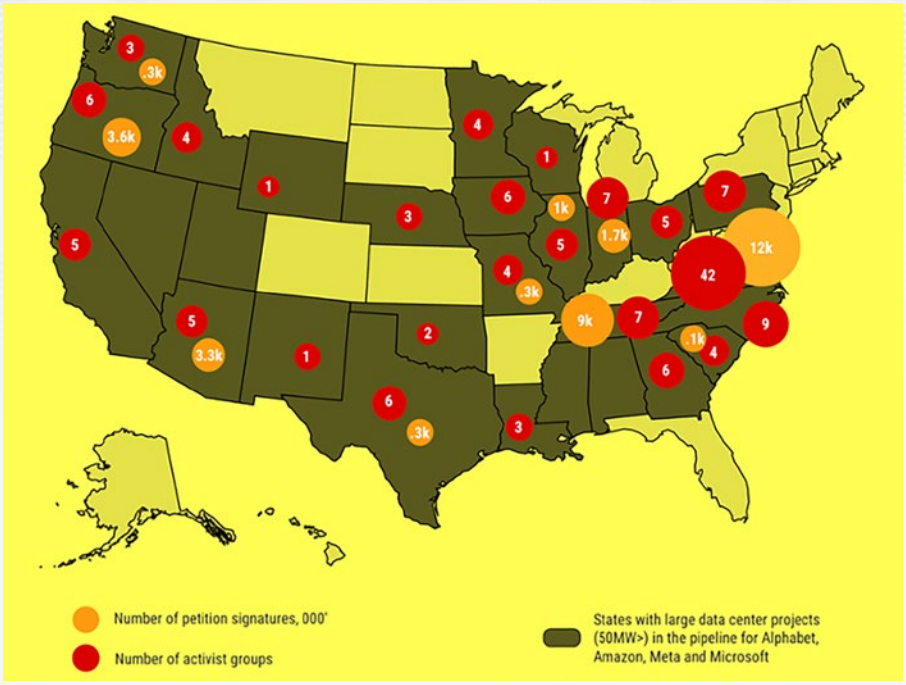
- The **American model** generally places greater emphasis on market-led innovation, private-sector scale, and competitive dynamism. Large technology firms play a central role, and public policy often prioritizes innovation capacity and national competitiveness.
- The **Chinese model** places greater emphasis on state coordination, strategic industrial policy, and direct control over data and digital platforms within a broader framework of political authority.
- The **European model** places relatively greater emphasis on rights-based governance, market regulation, interoperability, and accountability. At the same time, it operates within a more fragmented technological landscape and with more limited control over some of the largest global platforms and infrastructures.

These are broad tendencies rather than rigid categories, and each model contains internal variation. Still, they help explain why debates around sovereignty, innovation, and regulation often take different forms across regions.

This difference is visible in the regulation of artificial intelligence. In the United States, parts of the policy debate have focused on avoiding regulatory fragmentation and preserving innovation speed. In Europe, the AI Act reflects a stronger emphasis on legal clarity, risk classification, and public safeguards. At the same time, some European technology firms[27] have argued that implementation should be paced carefully to avoid undermining innovation or competitive position. These debates show that sovereignty also involves trade-offs between regulation, market development, and technological ambition.

[26] Aktoudianakis, A. (2020, December). *Digital sovereignty for growth, rules and cooperation*. European Policy Centre / Konrad-Adenauer-Stiftung. http://epc-web-s3.s3.amazonaws.com/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf

[27] Volpicell, G. (2025, July 3). *ASML, Airbus, Mistral Ask EU to Delay Start of AI Act Rules*. Bloomberg. https://www.bloomberg.com/news/articles/2025-07-03/asml-sap-mistral-ask-eu-to-delay-start-of-ai-act-rules



The map shows the geography of emerging negative reactions to data centres and how they relate to states where Amazon, Google, Meta and Microsoft (hyperscalers) have data centre projects of 50 MW> in the early planning stages.[29]

Sovereignty beyond institutions

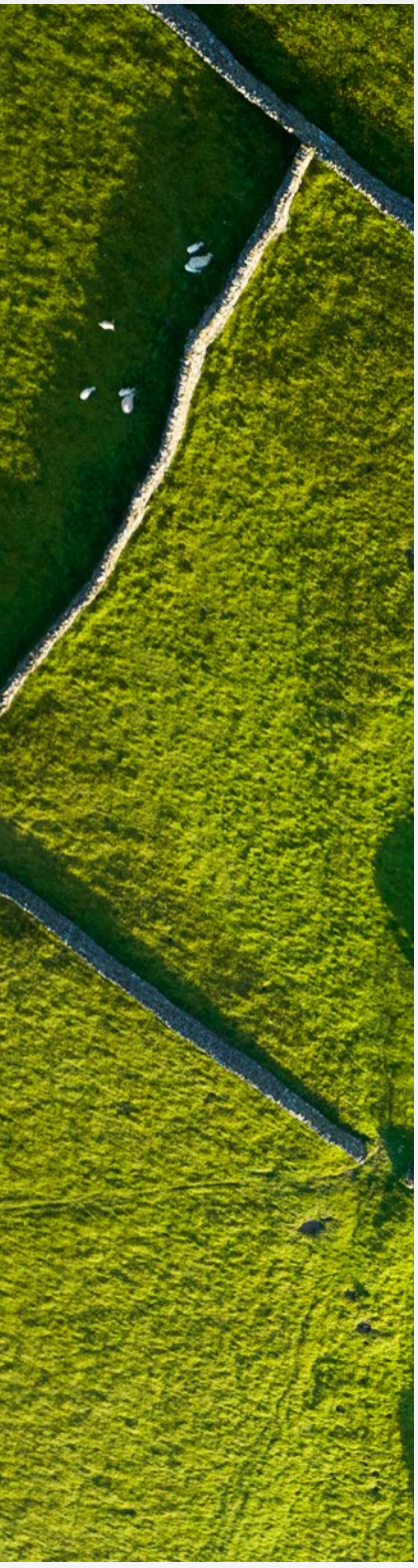
Although sovereignty is often discussed in terms of states and regulation, the topic increasingly extends to citizens, consumers, and local communities.

In Europe, consumer interest in European digital services and products has grown in some circles, reflecting broader concerns about privacy, legal jurisdiction, and dependence on large non-European platforms. Some online communities have framed purchasing and platform choices as a way of expressing preference for regional control or alignment with European norms. These developments suggest that sovereignty concerns are no longer confined to governments and boardrooms.

In the United States, public resistance to large-scale technology infrastructure has also grown, though often for different reasons. In some regions, local communities have raised concerns about the environmental and infrastructural impact of data centres, especially in relation to energy demand, water usage, land allocation, and electricity costs.

These debates are generally less about jurisdictional control and more about resource allocation, local autonomy, and the material footprint of digital infrastructure. In the state of Virginia, for example, more than a quarter of total electricity consumption is already attributed to data centres. As demand for power, water and land accelerates, local communities increasingly find themselves competing with hyperscale infrastructure for scarce resources. The consequences are tangible. Rising energy demand from the data centre sector is pushing up electricity prices and straining regional grids, while water usage and land allocation have become politically sensitive issues. According to Datacenter Watch,[28] between March 2024 and March 2025, an estimated $64 billion worth of data centre projects were delayed or blocked due to local opposition. In a survey covering 28 US states with planned data centres consuming 50 megawatts or more, the organisation identified 142 activist groups actively resisting these developments.

Taken together, these developments show that sovereignty is also appearing in debates about consumer choice, local consent, infrastructure planning, and the social costs of digital scale.



Conclusion

The concept of sovereignty has changed significantly since its early formulation in European political thought. What began in Westfalia as a principle associated primarily with territorial authority now extends into the digital domain, where control over infrastructure, data, platforms, standards, and technological capabilities increasingly shapes room for economic, institutional, and political decision-making.

A useful interpretation of sovereignty is practical and relational: sovereignty concerns the degree of control an actor retains over critical systems, the extent of acceptable dependency, and the ability to act when those systems are under pressure.

Different regions approach this challenge in different ways. Some prioritize speed, scale, and innovation. Others emphasize state coordination or legal control. Europe's contribution to the debate has been to stress accountability, rights, and proportional governance, while also confronting its own structural dependencies in key parts of the digital stack.

For organisations, the challenge is therefore not to pursue sovereignty as an abstract ideal, but to make deliberate choices about where control is essential, where resilience must be strengthened, and where interdependence remains entirely workable. Understood in this way, digital sovereignty is less a destination than a discipline: a way of thinking clearly about control, dependency, and strategic optionality in an increasingly digital world.

The definitions may be clear, but the implications are only beginning to unfold. In the next chapter we move beyond formal authority to explore the softer, less visible forms of power that increasingly shape sovereignty in the digital era.

[28] Data Centre Watch. (2025). *$64 billion of data centre projects have been blocked or delayed amid local opposition.* https://www.datacenterwatch.org/report

[29] Ibid.

Chapter 3
Technology as soft power

On 18 November 2025, major Dutch media organisations, both public and private, sent a letter to the exploratory negotiator involved in the formation of a new coalition government. In it, they expressed concern about the growing influence of global technology platforms on the Dutch information landscape.[30] Their argument was that this influence was affecting media pluralism, the visibility of domestic journalism, the preservation of Dutch cultural indentity and the conditions under which public debate takes place.

These concerns point to a broader question. Technology is often treated as a neutral instrument: a spreadsheet, an AI model, a collaboration platform, or a mail server can appear to be no more than a functional tool. In practice, however, digital technologies often reflect assumptions embedded in their design, governance, training data, interfaces, and business models. These assumptions may relate to efficiency, openness, moderation, privacy, hierarchy, language, worldview or commercial priorities. As a result, technologies do not simply enable action; they can also shape how people communicate, collaborate, interpret information, and make decisions.

Technology, then, is not a neutral tool, but a carrier of values and power. The real danger lies in its apparent invisibility. We adapt to its logic without noticing. Its influence is often subtle. It does not usually operate through direct coercion, but through defaults, incentives, interface design, and patterns of use that gradually become taken for granted. At the same time, technologies are not deterministic. Users, organisations, and societies can adapt, reinterpret, and repurpose them. The question is how much room remains to shape digital systems in ways that reflect local needs, institutional values, and cultural context.

From this perspective, digital sovereignty is not only about formal control over infrastructure or the ability to maintain access to markets. It is also about understanding which assumptions and priorities are embedded in the technologies that increasingly mediate communication, administration, and public life. In that sense, the issue is who defines the defaults.

[30] Stichting Democratie en Media. (2025, November 18). *Brief aan de informateur namens de Nederlandse mediasector.* https://sdm.nl/brief-aan-de-informateur-namens-de-nederlandse-mediasector/

AI and cultural context

This becomes particularly visible in artificial intelligence. Saskia Lensink, product manager of GPT-NL, the Dutch alternative to ChatGPT, offers a simple example. Ask an AI system to generate an image of someone eating ice cream on the beach. Depending on the system and the data on which it was trained, the result may reflect a particular set of cultural references: Miami Beach rather than Scheveningen (the beach close to The Hague, The Netherlands), American Blue Bunny, Dutch Ola or rather Indian Vadilal brand; one visual norm rather than another. The prompt may appear culturally neutral, but the output can still reflect dominant patterns in the training data.

Three images generated with ChatGPT. On the left, an American eating a Blue Bunny ice cream on a beach in Miami; in the middle, an Indian girl eating a Vadilal ice cream on Baga Beach; and on the right, a Dutch person eating an Ola ice cream on Scheveningen beach. Which image would you get if you entered the prompt "someone eating ice cream on the beach"? It shows that technology, and certainly an LLM, is a carrier of local culture.

This illustrates a broader point. Large language models and image generators do not simply retrieve facts. They generate outputs by reproducing patterns found in large datasets. In doing so, they may reflect certain languages, geographies, products, assumptions, and cultural norms more strongly than others. What appears central, typical, or "normal" in an AI system is often influenced by the data on which it was trained, the design choices made during development, and the commercial environment in which it operates.

For governments, public institutions, and organisations concerned with cultural representation, transparency, and control, this raises practical questions. To what extent should critical AI systems be locally adapted? How important is it that they are auditable? And under whose legal, linguistic, and operational framework should they function?

Some prominent AI researchers have argued that these questions justify greater investment in open and local models. Yann LeCun, Meta's former chief AI scientist, has been one of the most outspoken proponents of this position. "No country will have AI sovereignty without open-source models", he argues.[31] LeCun warns of a future in which countries become dependent on foreign AI they can neither fully inspect nor meaningfully control. His proposed remedy is unambiguous: each country, or region, should be capable of developing its own language models. The goal is to ensure that both the technology and the worldview it embodies remain subject to local values, oversight and democratic accountability.

In this light, training models on Dutch or European data can be understood as an attempt to improve relevance, accountability, and cultural fit. A model trained with attention to local language, law, institutions, and social context – from the difference between an Ola and a Blue Bunny ice cream to the political and social values that shape public life – may behave differently from a general-purpose system trained primarily on globally dominant data sources. For some use cases, especially in the public sector, that distinction may become increasingly important.

LeCun's argument, reinforced by Lensink's example, makes clear that digital sovereignty is not only about who can pull the plug, but about who defines what is considered "normal" in everyday interactions with technology. This is why investment in open, culturally grounded AI models is deemped so important by these critics. Such models preserve the ability of societies to see themselves reflected in the systems that increasingly mediate communication, decision-making, and meaning.

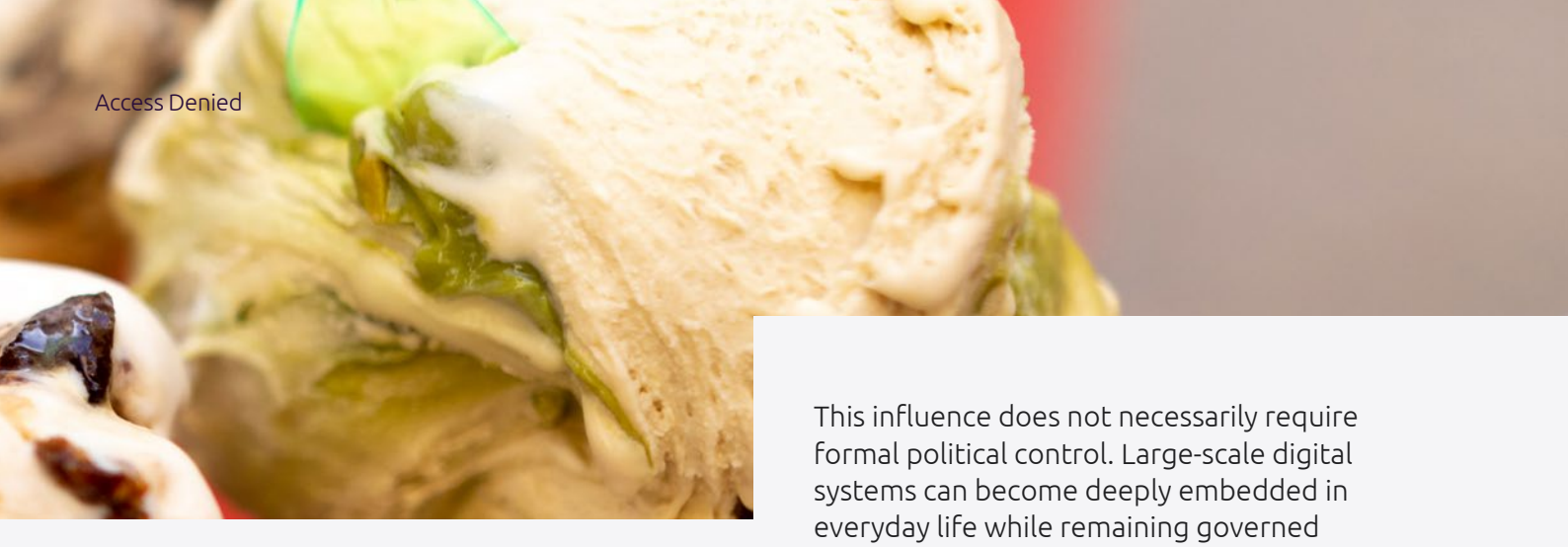
Sovereign AI as strategy and market

The growing interest in what is often called "sovereign AI" reflects this shift. The term is frequently used to describe AI systems that are trained, governed, hosted, or deployed in ways that provide countries or organisations with greater control over data, infrastructure, and oversight.

NVIDIA CEO Jensen Huang has described AI as a form of national infrastructure, comparable in some respects to telecommunications.[32] His argument is that as AI becomes integrated into public administration, economic coordination, research, security, and language services, governments will increasingly want direct influence over how these systems are built and operated. In practice, this may involve domestic data centres, regionally governed datasets, dedicated compute capacity, and deployment models aligned with local legal requirements.

[31] Snyder, G. (2025, April 2). Yann LeCun, Pioneer of AI, Thinks Today's LLM's Are Nearly Obsolete. *Newsweek*. https://www.newsweek.com/ai-impact-interview-yann-lecun-artificial-intelligence-2054237

[32] Gallagher, D. (2025, May 23). What the Era of 'Sovereign AI' Means for Chip Makers. *The Wall Street Journal*. https://www.wsj.com/finance/stocks/nvidia-ai-chipmakers-country-deals-05b5f44d



At the same time, the rise of sovereign AI is also creating a new commercial category. Companies that supply the hardware, cloud infrastructure, and software needed to build and operate AI systems are well positioned to benefit from this demand. In that sense, sovereign AI is developing both as a policy objective and as a market segment. Bank of America analyst Vivek Arya estimates that the market for so-called sovereign AI could ultimately reach $50 billion per year, accounting for roughly 10 to 15 percent of the global AI infrastructure market.[33] This dual character creates an important tension. The language of sovereignty can be adopted even when substantial parts of the underlying stack remain dependent on a small number of global providers. That does not make such initiatives meaningless, but it does raise questions about degree. How much control is actually achieved if models are hosted locally but run on external platforms, use externally supplied hardware, or depend on foreign software ecosystems? Sovereignty in AI, as in other domains, is likely to be partial rather than absolute.

Technology, influence, and soft power

These developments connect to a broader discussion about technology as a form of soft power. In international relations, soft power usually refers to the ability to shape the preferences, norms, or behaviour of others without direct coercion. In the digital context, this can occur when widely adopted platforms and infrastructures influence how people communicate, what information they encounter, which assumptions become normalized, and which actors gain privileged access to attention and data.

This influence does not necessarily require formal political control. Large-scale digital systems can become deeply embedded in everyday life while remaining governed elsewhere. Through search engines, social media platforms, mobile operating systems, advertising networks, and AI assistants, a relatively small number of organisations can shape the conditions under which public discourse, consumption, and institutional workflows take place.

A number of influential thinkers have described these developments in strongly critical terms. Historian Yuval Noah Harari, for example, argues in his latest book *Nexus* that the large-scale collection and analysis of data may create new forms of asymmetry in knowledge and influence. He calls this digital colonialism.[34] His concern is not simply that behaviour can be observed, but that digital systems may increasingly be used to anticipate and shape choices. The objective is to understand what people do, to grasp why they do it, and how to steer their next decision. In this reading, the concentration of data, compute, and algorithmic capability can produce a form of structural influence that is difficult to see but highly consequential. What makes this power historically unprecedented is AI's ability to participate directly in human communication: to intervene in conversations, generate narratives, and do so autonomously and at scale. As Harari has long argued, humans are storytelling beings. We interpret the world through stories and base our choices on their perceived credibility and coherence. This is precisely where the risk lies. Detailed behavioural insight – who we are, what we desire, what we fear –

is now fused with persuasive narratives produced by chatbots. The spectrum runs from the seemingly trivial, such as an innocent image of a Blue Bunny ice cream, to the profoundly consequential: a fabricated explanation of why a citizen should support a particular political party. In this convergence of intimate knowledge and automated persuasion, influence becomes subtle, scalable, and deeply effective. Much of this is no longer hypothetical; it is already occurring. This is the essence of what we call digital soft power.

Shoshana Zuboff has approached the issue from a related angle. In *The Age of Surveillance Capitalism*, she argues that behavioural data has become the basis of a new economic logic in which prediction and behavioural steering are central sources of value. Her emphasis is on the asymmetry between those who collect and process behavioural data at scale and those whose lives generate that data but who have little visibility into how it is used. Only a small number of corporations and states possess the scale, computing capacity, and advance models required to operate such markets. The rest of the world – citizens, small states, local businesses – functions primarily as a supplier of raw behavioural data, while remaining dependent on technologies designed, owned and governed elsewhere.[35]

Researcher and internet sceptic Evgeny Morozov extends this discussion into the cultural and cognitive domain. His concern is that sovereignty should not be understood only in legal or territorial terms, but also in terms of who shapes the epistemic environment in which people interpret reality. If digital systems structure what is visible, searchable, recommendable, and discussable, then the design of those systems becomes relevant to questions of autonomy and public reasoning.

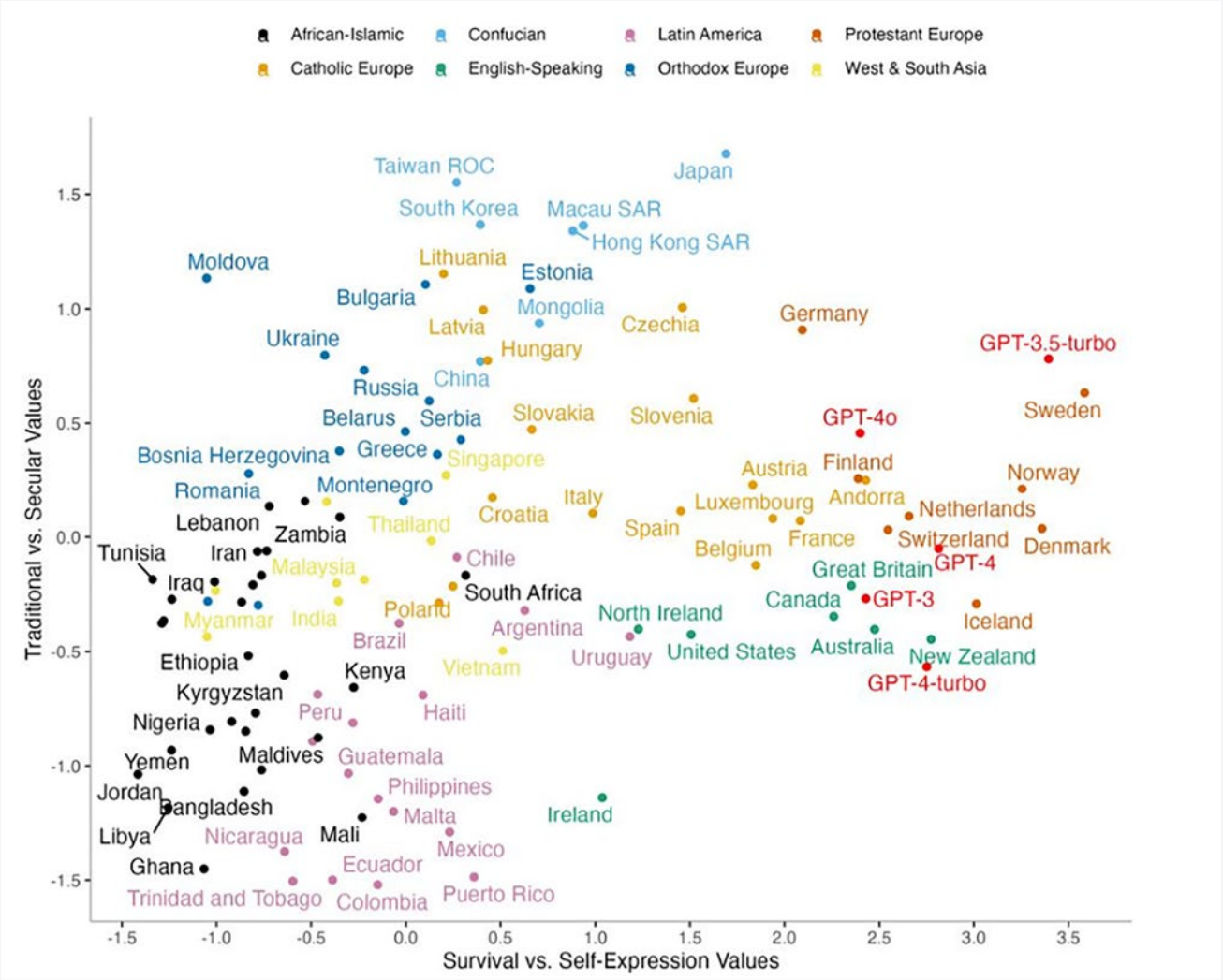
These perspectives differ in emphasis, but they converge on a common point: the concentration of digital infrastructure and intelligence systems can create asymmetries of influence that extend beyond economics alone. The issue is not just that technology determines behaviour in a simple way, but also that it can affect the conditions under which decisions are formed, information is prioritized, and social norms are reinforced.

That is where the concept of digital soft power becomes useful. It describes the ability of digital systems to shape environments of attention, expectation, and interpretation without relying on overt force. This influence may range from relatively minor forms of cultural default – such as which products, locations, or references are treated as standard – to more consequential effects in areas such as news distribution, political communication, education, or public administration.

[33] Tipranks (2025, May 16). Bank of America Names AMD a 'Top Winner' in Saudi Arabia's AI Push. *The Globe and Mail*. https://www.theglobeandmail.com/investing/markets/stocks/AMD/pressreleases/32434287/bank-of-america-names-amd-a-top-winner-in-saudi-arabias-aipush

[34] Harari, Y.N. (2024, August 24). 'Never summon a power you can't control': Yuval Noah Harari on how AI could threaten democracy and divide the world. *The Guardian*. https://www.theguardian.com/technology/article/2024/aug/24/yuval-noah-harari-ai-book-extract-nexus

[35] Nagovitch, P. (2025, December 15). Shoshana Zuboff, philosopher: 'AI is surveillance capitalism continuing to evolve and expand'. *El Pais*. https://english.elpais.com/technology/2025-12-15/shoshana-zuboff-philosopher-ai-is-surveillance-capitalism-continuing-to-evolve-and-expand.html



Language models are examined to determine what values they convey. With each new model and the interim tweaks that are made, norms and values shift. [36]

Cultural representation and institutional control

Seen in this way, the question of sovereignty is also about the ability to influence the representational and operational logic of digital systems. Which language is prioritized? Which institutional assumptions are built into workflows? Which legal framework applies? Which social norms are taken as default?

These questions become especially relevant when technology is widely used in public-sector environments such as education, healthcare, administration, and justice. A platform or AI system that works well in one jurisdiction may still reflect assumptions that are only partially aligned with another. For commercial consumer tools, that may be manageable. For systems used in sensitive or high-impact contexts, the issue becomes more significant.

This does not imply that all externally developed technology is unsuitable, nor that domestic or regional alternatives are automatically superior. It does suggest, however, that greater awareness is needed of the cultural, institutional, and operational assumptions that technologies may carry. In some cases, organisations may conclude that adapting existing tools is sufficient. In others, they may prefer systems that offer greater transparency, local relevance, or legal control.


Access Denied

From that perspective, initiatives such as GPT-NL can be understood not primarily as symbolic national projects, but as experiments in creating AI systems that are more closely aligned with local governance requirements, language context, and public accountability. Their significance lies less in technological isolation than in widening the range of available choices.

Conclusion

Technology is often discussed in terms of functionality, scale, and efficiency. Those dimensions matter, but they do not capture the full picture. Widely adopted digital systems can also influence which assumptions, norms, and references become embedded in everyday workflows, public communication, and institutional decision-making. In that sense, technology can function as a form of soft power.

It shows that technologies are never neutral in practice. Their design, training data, interfaces, and governance structures can shape the defaults within which individuals and organisations operate.

For that reason, debates about digital sovereignty increasingly extend beyond access and infrastructure. They also include questions of auditability, cultural relevance, legal oversight, and institutional fit. In artificial intelligence especially, these issues are becoming more visible as models are integrated into public services, economic processes, and daily communication.

The growing interest in sovereign AI should therefore be understood in this broader context. For some governments and institutions, developing or deploying more locally governed AI systems is one way to improve transparency, accountability, cultural representation, and operational control. At the same time, such efforts remain embedded in global supply chains and commercial ecosystems, which means sovereignty is likely to remain a matter of degree rather than a fixed condition.

The central issue, then, is whether societies, institutions, and organisations retain enough influence over the systems they depend on to ensure that those systems remain compatible with their values, responsibilities, and long-term interests.

[36] Tao, Y. et al. (2024, September 17). Cultural bias and cultural alignment of large language models. *PNAS Nexus*, *3*(9), 1-9. https://academic.oup.com/pnasnexus/article-pdf/3/9/pgae346/59151559/pgae346.pdf

Chapter 4
Building blocks for a sovereign Europe

Europe is beginning to wake up – and, cautiously, to act. At the request of Ursula von der Leyen, Italian economist and former ECB president Mario Draghi authored a landmark analysis on Europe's strategic future. In *The Future of European Competitiveness*, widely known as the "Draghi Report", he sets out a stark diagnosis. At its core lies a widening productivity gap with the United States, driven largely by Europe's delayed adoption and development of digital technologies:

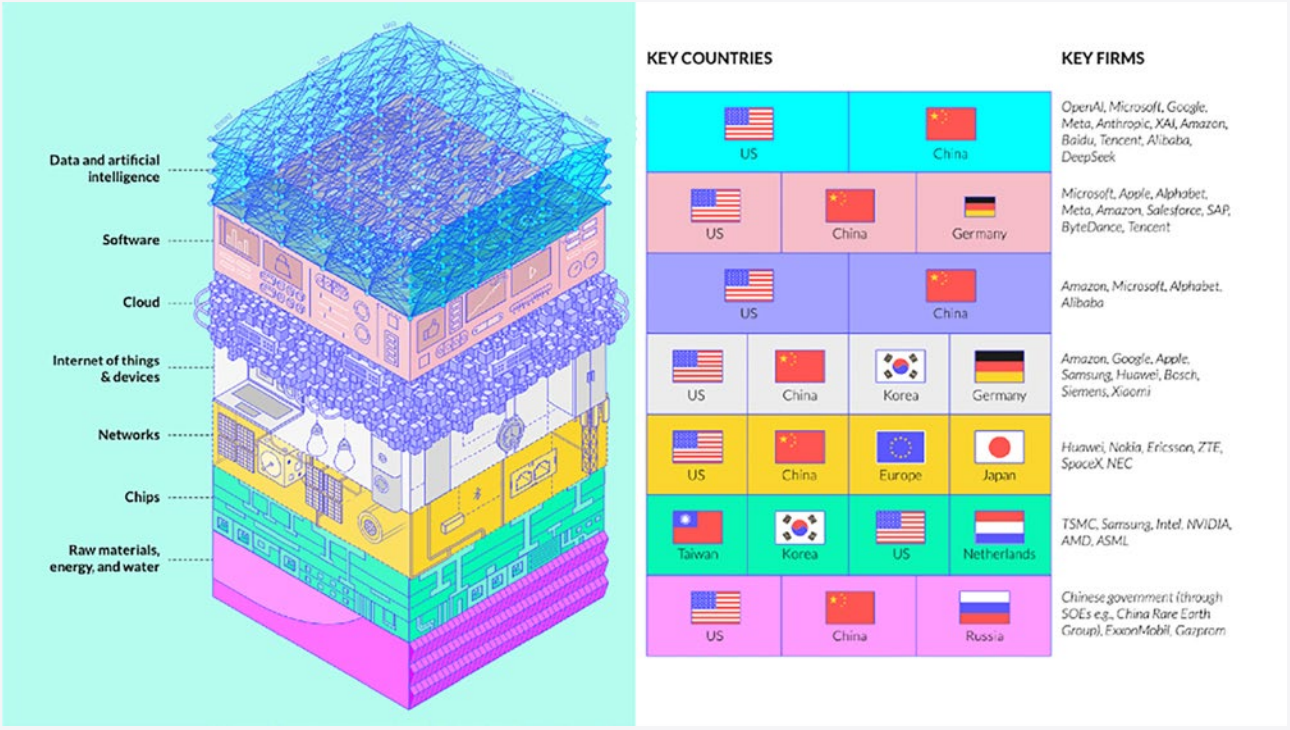
"The key driver of the rising productivity gap between the EU and the US has been digital technology ('tech'). Unless Europe acts now, the gap will widen further, undermining growth and resilience."[37]

While the United States and China are building integrated ecosystems around AI, semiconductors, and cloud infrastructure – fueled by scale, venture capital and assertive industrial policy – Europe continues to lag, constrained by fragmentation and caution. Since 1995, labour productivity in the United States has grown at an average of 1.8 percent per year, compared with just 1.1 percent in the EU. Draghi attributes much of this gap to Europe's slow pace of digital adoption and chronic underinvestment in emerging technologies.

A moment of truth is approaching. Does Europe commit to large-scale, coordinated industrial policy – or does it persist in fragmented, incremental investment? The Draghi Report is unequivocal: digital sovereignty is not a luxury, but a prerequisite for competitiveness. Europe must:

1. reduce strategic dependencies (cloud, semiconductors, satellites, telecommunication);
2. create scale through a Digital Single Market;
3. develop sovereign solutions (cloud, data, defence) to protect critical infrastructure.

[37] Draghi, M. (2024, September). *The future of European competitiveness: Part A | A competitiveness strategy for Europe.* European Commission. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The+future+of+European+competitiveness+_+A+competitiveness+strategy+for+Europe



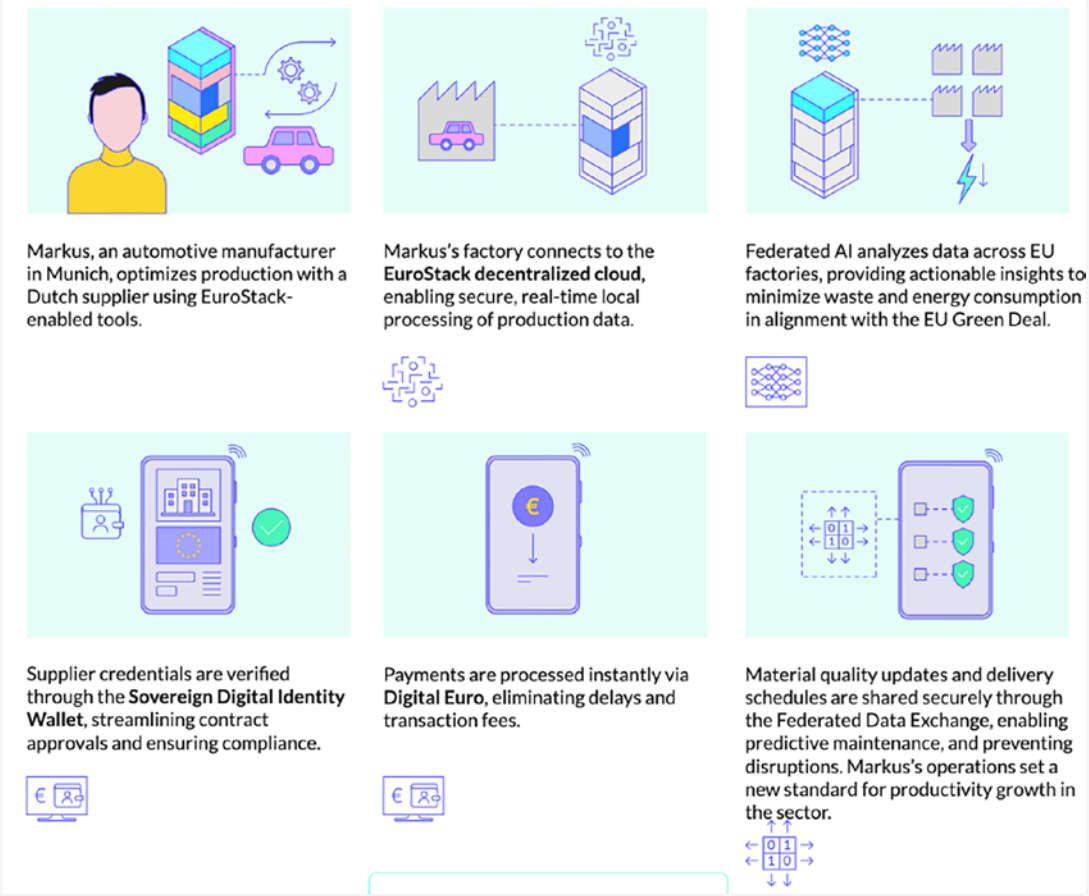
There is a vision and additional funding is on the way. Yet, the report also makes clear that Europe is starting from an uneven position. In several strategic technology domains, including cloud infrastructure, AI, and satellite communications, Europe has important assets but limited scale relative to larger ecosystems elsewhere. Europe's planned IRIS² satellite system, for example, has been cited as an effort to strengthen communications resilience and strategic autonomy, while also illustrating the challenge of moving from ambition to implementation at sufficient speed and scale.

Further initiatives are likely in the coming years. Whether these efforts ultimately produce a more coherent European technology landscape will depend on coordination, sustained investment, interoperability, procurement choices, and the extent to which organisations see practical value in the alternatives being developed. This chapter reviews a number of initiatives and companies that illustrate how parts of this landscape are beginning to take shape

The EuroStack

One useful framework for understanding the emerging European technology landscape is the EuroStack. Developed by a group of European thinkers, entrepreneurs, and policymakers, the concept outlines a strategic approach to strengthening Europe's capabilities across multiple layers of the digital stack. It is associated in particular with the work of innovation economist Francesca Bria and has been discussed as a way of reducing structural dependencies while reinforcing Europe's capacity to shape its own digital infrastructure and services.

The EuroStack framework is broad by design. It spans semiconductors, networks, IoT, cloud infrastructure, software platforms, data, and artificial intelligence. The framework gained visibility in 2025, at a time when questions of technological dependency, industrial policy, and digital governance were receiving increased attention across Europe. Support for the broader EuroStack agenda has come from a range of actors, including technology companies, academic voices, and parts of the European policy community. Its prominence also reflects the extent to which digital capability has become a more central issue in discussions about Europe's competitiveness and long-term resilience.



An example of an MVP from the EuroStack report in which efficiency, resilience and sustainability are paramount.

A notable aspect of EuroStack is its layered view of technological power. It draws attention to different levels of the stack, each with its own dependencies, capabilities, and policy challenges. At certain layers, Europe has visible strengths – for example in semiconductor equipment, industrial software, and parts of the open-source ecosystem. At other layers, it remains more dependent on external providers. In the report all this is visualised with a striking digital world map.

The framework is also linked to several policy preferences. These include stronger support for open-source technologies, greater interoperability, investment in shared digital services, and procurement models that may give more weight to European providers where this is strategically justified.

Some proposals associated with EuroStack also emphasize demonstrator projects such as digital identity infrastructure, payments, and trusted data-sharing environments as ways to translate strategic ambition into operational capability.

In the area of artificial intelligence, EuroStack places particular emphasis on strengthening European model development, data infrastructure, and deployment options. The reasoning is that AI increasingly affects multiple sectors at once and therefore influences not only innovation capacity, but also administrative systems, industrial processes, and public services. Within this framing, AI is seen as one of the layers where improved optionality and governance capacity may have wider systemic effects.

As the authors state:

"Artificial intelligence (AI) is the cornerstone of the EuroStack vision and offers unparalleled opportunities to transform Europe's digital ecosystem. The revolutionary potential of AI extends across all sectors, from manufacturing and healthcare to public services and energy management. By investing in sovereign AI ecosystems, Europe can operate more efficiently, create smarter public services and stimulate indigenous innovation that aligns with European values such as transparency, accountability and privacy."

In this context AI is more than just another technology layer – it is the lever through which Europe can translate values into capability, and ambition into lasting strategic relevance.

Realising this vision would require substantial long-term investment. Proposals linked to EuroStack include large-scale public and private financing, including the possible creation of dedicated European funding structures to support shared technology capabilities. Whether such proposals are implemented at the necessary scale remains uncertain, but they illustrate the level of ambition that some advocates believe is required.

At the same time, the framework also highlights an enduring European challenge: translating strategic intent into coordinated execution across multiple countries, institutions, and markets. In that respect, the relevance of EuroStack lies not only in the specific measures it proposes, but also in the broader question it raises: how can Europe combine openness with sufficient control over critical parts of its digital environment?

Digital pioneers

Across Europe, a new generation of technology companies is emerging. Together, they reflect a growing set of design choices across different layers of the digital stack: cloud infrastructure, AI models, data platforms, governance frameworks, and digital services. These initiatives should not be read simply as alternatives to existing global providers, but as attempts to strengthen particular layers of control within an evolving European digital ecosystem. No single actor currently offers complete sovereignty across infrastructure, software, AI models, governance and industrial scale. Each initiative addresses specific dependencies while leaving others intact. Some strengthen jurisdictional control, others focus on transparency, operational accountability, open architectures, or sector-specific trust requirements.

What makes many of these initiatives notable is that they often embed concerns such as data sovereignty, public accountability, transparency and regulatory alignment more explicitly into their design choices. At the same time, this landscape remains uneven: fragmented in places, early-stage in others, and still developing in industrial scale.

Its strategic relevance therefore lies less in identifying a preferred provider category than in understanding which layer of control each initiative strengthens, where limitations remain, and in which contexts these solutions become meaningful.

Taken together, these companies help sketch the early contours of a European digital ecosystem. Still incomplete, but increasingly visible as part of a broader sovereignty landscape. Below is a selection of European initiatives that illustrate how this next phase is beginning to take shape.

STACKIT: industrial cloud capacity within a European jurisdiction

STACKIT, part of Schwarz Group through Schwarz Digits, represents one of the more substantial European initiatives in sovereign cloud infrastructure. Originally developed to support the internal IT requirements of Lidl, Kaufland and other Schwarz Group activities, it has gradually evolved into a cloud provider serving external enterprise customers, initially in Germany and Austria. Its strategic relevance lies primarily in infrastructure ownership and jurisdictional control: services are hosted within Germany and Austria, with strong emphasis on data protection, regulatory compliance, and operational transparency under European legal frameworks.

At the same time, STACKIT operates in a market where industrial scale, platform breadth, and ecosystem maturity remain decisive competitive factors. Compared with global hyperscalers, its portfolio is still narrower, particularly in advanced platform services and international reach.

Rather than functioning as a direct substitute for hyperscale cloud providers, STACKIT illustrates how European actors can strengthen sovereignty in selected layers of the cloud stack, especially where jurisdiction, operational control and local trust requirements carry particular weight.

Its longer-term ambition to expand further reflects a broader European effort to increase strategic optionality in cloud infrastructure without assuming that all dependencies can or should disappear.

AMI Labs: research-driven AI models from Paris

In the wake of growing European activity in AI model development, AMI Labs (Advanced Machine Intelligence), founded in Paris in late 2025 by Yann LeCun following his departure from Meta, represents a recent addition to the landscape. The company focuses on developing so-called "world models", which aim to capture aspects of physical reality and causal relationships, complementing existing approaches that are primarily centred on text-based prediction.

This research direction reflects broader exploration within the AI field into alternative model architectures and capabilities beyond current large language models. AMI Labs' work is therefore positioned within a wider international effort to expand the scope of AI systems toward more structured reasoning and interaction with real-world environments.

The initiative has attracted attention from public and private stakeholders in France and at European level, reflecting interest in strengthening research and development capacity in emerging areas of AI. In March 2026, AMI Labs raised $1.03 billion in a seed round, one of the larger early-stage financings in this domain.

In this context, AMI Labs contributes to the diversification of approaches within the AI ecosystem, particularly in areas where different model paradigms may complement existing capabilities and support a broader range of use cases.[38]

Nscale: AI infrastructure provider with British and Nordic roots

The company, which emerged from the infrastructure arm of Arkon Energy in 2024, operates across multiple layers of AI infrastructure: from data centres (including a large-scale AI facility in Glomfjord, Norway) to specialised orchestration software. In March 2026, Nscale raised $2 billion in a Series C round – one of the largest equity financings in European technology – valuing the company at $14.6 billion. With support from investors such as NVIDIA, Dell Technologies and Aker ASA, Nscale provides high-performance GPU computing capacity for organisations with demanding AI workloads.

Its positioning reflects growing demand for infrastructure options that allow organisations to consider factors such as workload placement, regulatory context, and operational control alongside performance and scale. In this context, Nscale contributes to expanding the range of available infrastructure configurations within an increasingly diverse and globally interconnected AI ecosystem.[39,40]

---

[38] French Tech Journal. (2026, March 3). *AMI Labs raises record $1B seed round to challenge Silicon Valley's AI dominance.* https://frenchtechjournal.com/ami-labs-funding-billion

[39] Nscale Press. (2026, March 9). *Nscale Raises $2 Billion in Series C — the Largest in European History.* https://www.nscale.com/press-releases/nscale-series-c

[40] EU-Startups. (2026, March 9). *Nscale secures €1.7 billion Series C to build global AI compute infrastructure.* https://www.eu-startups.com/2026/03/nscale-secures-e1-7-billion-series-c-to-build-global-ai-compute-infrastructure/

Nextcloud: open-source collaboration platform for controlled deployment

While discussions around cloud sovereignty often focus on infrastructure, Nextcloud (based in Berlin and Stuttgart) represents a widely used approach at the software layer. The platform provides an open-source collaboration environment covering file sharing, communication and productivity functions, and can be deployed in different configurations depending on organisational requirements.

Organisations using Nextcloud can choose where and how their data is hosted – whether on-premise or through regional service providers such as KPN or IONOS. This flexibility allows alignment with specific needs related to data governance, compliance, and operational control.[41]

The platform is used across a range of European public-sector environments, including initiatives such as the Bundescloud and deployments within the French National Gendarmerie. In The Netherlands, it is also deployed through organisations such as SURF to support collaboration in education and government contexts.

In this context, Nextcloud contributes to expanding the range of software deployment models available to organisations, particularly in scenarios where hosting flexibility, transparency and integration into existing environments are relevant considerations.

Lovable: prompt-based application development

Lovable, founded in Stockholm in 2023, illustrates a different layer of Europe's evolving digital landscape: not infrastructure, but software creation through AI-assisted code generation. The company has gained rapid visibility with a platform that enables users with limited programming expertise to generate applications through natural-language prompts.

Its growth trajectory has been notable, with strong investor attention and rapid commercial adoption.[42,43] The platform integrates with widely used developer environments such as GitHub and Supabase, while emphasising privacy terms, code ownership clarity, and hosting arrangements aligned with European data expectations.

What distinguishes Lovable is less jurisdiction than product design. Rather than producing isolated code fragments, the platform generates complete, functioning agents that combine frontend, backend and database components in a single workflow. This reflects a wider movement in software engineering in which increasing abstraction allows non-specialists to participate more directly in application creation.

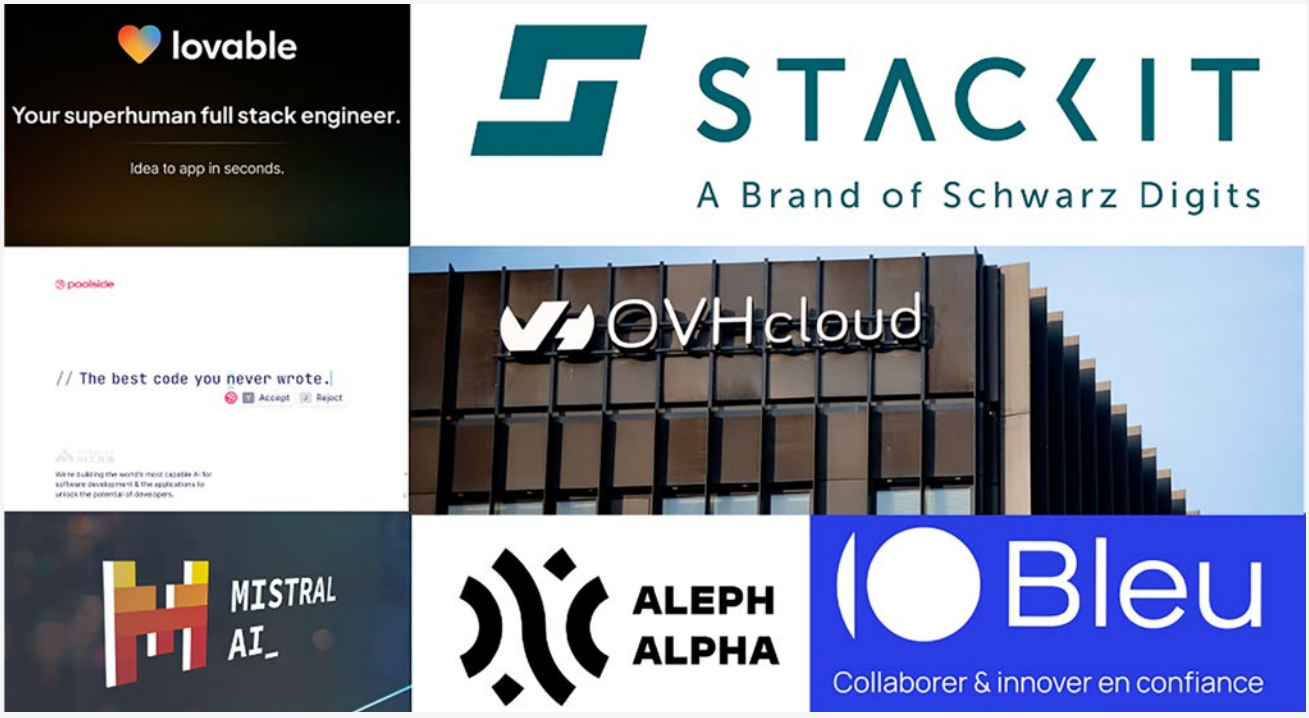
Its rapid rise illustrates that sovereignty in digital ecosystems is not only shaped at the infrastructure level, but also through companies that strengthen optionality, capability and innovation in specific parts of the software stack.

---

[41] Spinner, Y. (2026, February 22). *Europa wil weg van Microsoft 365 en Nextcloud ligt voor de hand*. https://tweakers.net/reviews/14376/europa-wil-weg-van-microsoft-365-en-nextcloud-ligt-voor-de-hand.html

[42] Lovable (2025, December 25). *Lovable raises $330M to power the age of the builder.* https://lovable.dev/blog/series-b

[43] Matthews, J. (2025, July 3). *Swedish AI startup Lovable rockets to £2bn valuation with £150m mega-round*. TFN. https://techfundingnews.com/lovable-raises-150m-growth-round



Europe has a range of options, from cloud providers to innovative AI start-ups.

Mistral AI: open models within Europe's AI landscape

Within Europe's emerging AI landscape, Mistral AI – founded in Paris in 2023 – has rapidly become one of the most visible European actors in large language models. With a strong emphasis on open models, scientific transparency and technical accessibility, the company has gained international prominence in a relatively short period of time. In less than a year, it raised more than €500 million in growth capital and reached a valuation exceeding €6 billion, reflecting strong market confidence in Europe's capacity to participate meaningfully in frontier AI development.

A defining characteristic of Mistral is its explicit commitment to openness. Model weights and technical details behind systems such as Mistral 7B and Mixtral have been made publicly available to a degree uncommon among leading frontier model providers. This allows companies, public institutions and research organisations to deploy, adapt and audit models locally, depending on their own infrastructure and governance requirements.

However, openness does not remove all dependencies. Training, deployment and large-scale industrial adoption remain linked to broader compute availability, cloud infrastructure and ecosystem choices that extend beyond Europe. The significance of Mistral therefore lies less in complete technological autonomy than in strengthening optionality at the model layer: offering an additional path for organisations that value inspectability, flexibility and local control.

Equally important is the ecosystem around the company. Mistral collaborates with a range of infrastructure and cloud partners, including European actors, and contributes to a broader discussion about how model development, deployment and governance can be organised under different regulatory and operational assumptions.

In that sense, Mistral is not only relevant as a technology company, but also as an example of how Europe is seeking to strengthen selected capabilities within the AI stack without assuming that all dependencies can disappear.

That strategic relevance became more visible in September 2025, when ASML acquired an 11 percent stake in Mistral for €1.3 billion. The investment reflects growing interest in connecting European strengths across hardware, infrastructure and AI development, while recognising that competitiveness in this domain depends on long-term industrial coordination rather than isolated initiatives.

ZenDiS: orchestration for public-sector digital sovereignty

ZenDiS attracted wider international attention in early 2025 when it was referenced in discussions following a temporary access incident involving the office of Karim Khan at the International Criminal Court in The Hague. The episode drew renewed attention to a broader question increasingly relevant to public institutions: how operational continuity, governance and digital dependencies are organised in critical institutional environments.

ZenDiS was established by the Germany federal government with the explicit mandate to strengthen digital sovereignty across national, state and municipal public administration.[44] Operational since 2024, it functionsless as a traditional technology vendor and more as an orchestration layer: selecting, bundling and supporting open-source solutions from commercial providers, including Nextcloud, and making them available to public institutions through an integrated delivery model.

These components are combined into a unified platform intended to simplify adoption, governance and operational consistency for public-sector users. Among its larger users is the Robert Koch Institute, Germany's national public health authority.[45]

ZenDiS illustrates one possible approach to digital sovereignty in practice: not by developing every component independently, but by organising existing technologies into a framework where transparency, auditability and governance requirements can be addressed more coherently within the public sector.

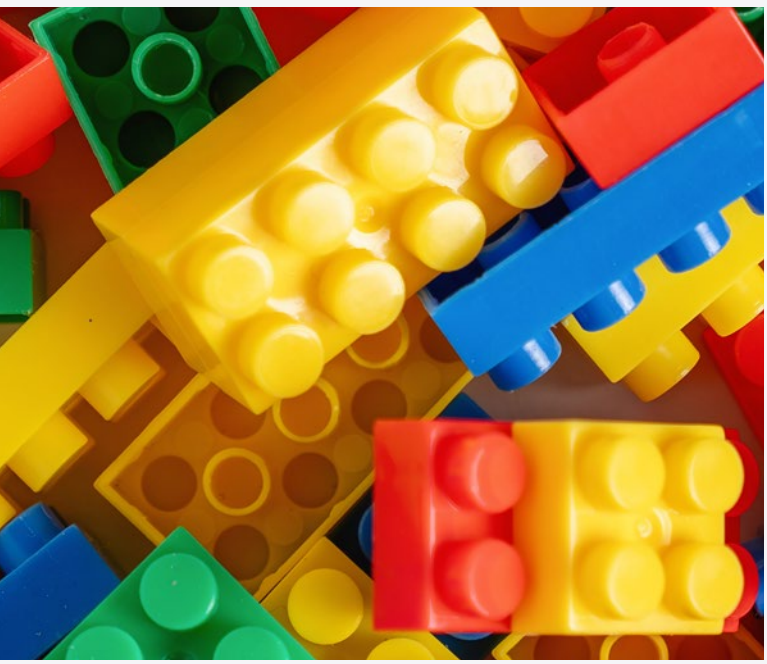
[44] ZenDiS. (n.d.). *Unser Auftrag*. https://www.zendis.de/unser-auftrag

[45] Eijsvoogel, J. (2025, November 4). Internationaal Strafhof dumpt Microsoft en kiest voor Europees alternatief. *NRC*. https://www.nrc.nl/nieuws/2025/11/04/internationaal-strafhof-dumpt-microsoft-en-kiest-voor-europees-alternatief-a4911821

Aleph Alpha: explainability and controlled deployment in generative AI

Aleph Alpha, founded in Heidelberg in 2019, was among the early European companies to position itself in large language models with a particular focus on explainability, traceability and auditability. Rather than competing primarily on model scale, the company has concentrated on architectural characteristics that support interpretability and controlled deployment.

This positioning has made Aleph Alpha particularly relevant in domains where trust, compliance and operational assurance carry significant weight, including public administration, defence-related environments, healthcare and legal contexts. The company increasingly presents itself not only as a model provider, but as a broader generative AI technology stack designed for integration into environments where governance requirements are high.



Its models are accessible through open APIs, while also allowing deployment on-premise or within controlled infrastructures. This flexibility enables organisations to integrate generative AI in ways that align with specific operational, legal or security requirements, depending on the context in which the models are used.

Aleph Alpha's role should also be understood against the backdrop of an AI field where compute capacity, model evolution and industrial adoption are increasingly concentrated at global scale. Its contribution lies in expanding the range of available choices for organisations that need transparency, operational control and regulatory assurance.

In 2023, the company secured €500 million in funding from a consortium including Bosch, SAP and German public investment actors.[46] The investment reflected broader interest in reinforcing European capabilities in selected parts of the AI stack, particularly where industrial use, trust and governance converge.

TildeOpen LLM: multilingual model development within European infrastructure

TildeOpen LLM, developed by Tilde with support from the European Commission and trained on the LUMI in Finland, represents one of the more visible European efforts in multilingual large language models. The model comprises 30 billion parameters and is optimised for all 24 official EU languages, alongside Ukrainian, Norwegian and several Balkan languages.[47]

It builds on Tilde's longer-standing expertise in language technology and machine translation for Europe's linguistically diverse markets.[48] Supported through European AI funding programmes and trained using more than two million GPU hours, TildeOpen reflects a broader effort to strengthen model development around linguistic diversity and regional language coverage. Areas that are often less central in globally dominant language models.

A notable characteristic of the model is its explicit focus on multilingual support, documentation, traceability and regulatory alignment. Data provenance, auditability and risk classification are documented in line with European regulatory expectations, while storage and inference are organised within European infrastructure.

In that sense, TildeOpen illustrates how specific European priorities, particularly linguistic diversity, documentation and governance, can be more explicitly reflected in model design choices.

Nebius: AI cloud infrastructure with European relevance

In the Dutch tech landscape, Nebius occupies a prominent position. Based in Amsterdam and listed on the Nasdaq, this fast-growing technology company has evolved from an emerging player into a billion-dollar enterprise active in the field of cloud and AI infrastructure.

Nebius is building a highly integrated cloud and AI platform that spans multiple layers of the stack: from large-scale GPU clusters to software and development tools for AI applications.

This infrastructure is designed to provide start-ups and enterprises with an additional option for running data-intensive AI workloads, particularly in scenarios where considerations such as infrastructure control, workload placement, or ecosystem diversification play a role. Like other emerging providers in this space, it contributes to expanding the range of design choices available within an evolving AI and cloud landscape.

[46] Partington, M. (2023, November 6). *Aleph Alpha raises $500m Series B in one of Europe's largest AI rounds ever.* Sifted. https://sifted.eu/articles/ai-startup-aleph-alpha-raises-500m

[47] Europese Commissie. (2025, September 9). *Door de EU gefinancierde TildeOpen LLM levert Europese AI-doorbraak voor meertalige innovatie.* https://digital-strategy.ec.europa.eu/nl/library/eu-funded-tildeopen-llm-delivers-european-ai-breakthrough-multilingual-innovation

[48] Tilde. (n.d.). [About Tilde]. https://tilde.ai/about-tilde/

Euclyd: specialised chip design for AI workloads

Euclyd, a Dutch startup founded by Bernardo Kastrup, focuses on the design of chips specifically optimised for AI workloads. Rather than relying on general-purpose architectures, the company explores approaches tailored to particular computational patterns associated with machine learning and inference tasks.

This design strategy reflects a broader trend in the semiconductor landscape, where specialised hardware is increasingly developed to complement general-purpose processors. In certain use cases, such targeted architectures can deliver significant improvements in efficiency and performance compared to more generic solutions, depending on workload characteristics and deployment context.

Euclyd's work highlights how innovation in chip design can contribute to diversifying the technological options available within the AI stack. Like other initiatives in this domain, it addresses specific aspects of the infrastructure layer while remaining part of a globally interconnected semiconductor ecosystem.[49]

Poolside: AI-assisted software development for professional engineers

Poolside is a French-American AI startup founded in Paris with a clear focus on software development supported by generative AI. Where platforms such as Lovable are oriented toward no-code and low-code application creation, Poolside is positioned more directly toward professional software engineers seeking to accelerate coding, testing and maintenance with AI acting as a true pair programmer.

What distinguishes the company is its emphasis on models designed specifically for code-related tasks, combined with its own developer interface intended to support deeper contextual interaction during software development. This places Poolside in a part of the AI landscape where specialised model behaviour and developer tooling increasingly converge.

Its positioning also reflects growing attention to issues such as data handling, deployment control and enterprise integration, particularly for organisations that want AI support in software engineering without fully standardising on external developer platforms.

In 2024, Poolside raised $126 million in an early investment round led by Air Street Capital and Bpifrance, with participation from Eric Schmidt and other investors.[50] The round illustrates continued investor interest in European-linked AI ventures operating in technically specialised domains. For Europe, Poolside is relevant not as a separate software stack, but as an example of how companies active in developer productivity and infrastructure tooling can contribute to strengthening capability in parts of the digital ecosystem that remain strategically important yet often less visible.

[49] Kastrup, B. (2026, January 5). *Europe's last hope in the AI race.* Iai News. https://iai.tv/articles/europes-last-hope-in-the-ai-race-auid-3453#:~:text=Many%20believe%20that%20our%20only,what%20Europeans%20consider%20fair%20and

[50] NewsnReleases. (2023, August 24). *Code-writing AI startup Poolside raises $126m and moves to Paris.* https://newsnreleases.com/2023/08/24/code-writing-ai-startup-poolside-raises-126m-and-moves-to-paris

GPT-NL: public AI for public values

GPT-NL is a distinctive initiative within The Netherlands: the first publicly funded large language model projects developed through a consortium including TNO, SURF, the Netherlands Forensic Institute and the Dutch AI Coalition. Its objective is to develop a language model with strong emphasis on transparency, explainability and alignment with European legal and regulatory frameworks, trained on Dutch-language data and accessible to public-sector, research and societal organisations.

Rather than focusing primarily on scale or broad commercial deployment, GPT-NL concentrates on use cases where public accountability, linguistic specificity and governance are central design considerations. The models are hosted by SURF, run on European infrastructure, and are developed in a way that allows external review and technical scrutiny.

What truly sets GPT-NL apart is its explicit treatment of AI as a public good. It reflects the conviction that certain forms of digital infrastructure – including foundational AI – should be partially publicly owned and governed, much like railways, electricity grids or public healthcare systems. In doing so, GPT-NL moves beyond principles to practice, offering a concrete example of how values such as transparency, fairness and inclusivity can be embedded into AI systems – and how public institutions can reclaim agency in an AI-driven world.

OVHcloud: large-scale cloud infrastructure under European jurisdiction

OVHcloud is Europe's largest cloud company and one of the continent's most established infrastructure providers. Founded in Roubaix, the company has grown into a global operator, running more than 400,000 servers and operating data centres in 140 countries worldwide.

Its relevance within the European digital landscape lies largely in the combination of industrial scale and jurisdictional positioning. OVHcloud operates under European legal frameworks and builds much of its offering around open-source technologies, infrastructure control, and operational transparency. Characteristics that are particularly relevant for organisations with stronger regulatory, compliance or governance requirements.

Compared with global hyperscalers such as Amazon Web Services and Microsoft Azure, OVHcloud's portfolio reflects a different balance between scale, platform breadth and legal environment. For some organisations, that creates an additional option where infrastructure location, legal jurisdiction and chain-of-control are considered important design criteria.

OVHcloud has also taken an active role in European cloud policy discussions. In 2021, together with several partners, it filed a formal complaint with the European Commission concerning cloud market practices and competition conditions. This reflected both commercial positioning and a wider debate within Europe about how cloud markets should evolve in relation to openness, competition and strategic resilience.

In that sense, OVHcloud illustrates a broader development in Europe's cloud landscape: alongside continued use of global hyperscale infrastructure, regional providers are seeking to strengthen control, and optionality within selected parts of the digital stack.

Bleu: a French sovereign cloud

Bleu is the joint response of Capgemini and Orange to the growing demand for cloud solutions that combine hyperscale capability with stronger European control. The platform delivers Microsoft Azure-based cloud services, but does so under strict French governance: operated by a French entity, hosted exclusively on French soil, and governed within a legal and operational framework designed to meet French and European sovereignty requirements while limiting exposure to extraterritorial risk.

Bleu is explicitly designed for critical and highly regulated sectors, including government, defence-adjacent services, and healthcare. A central objective is certification under ANSSI's SecNumCloud framework, France's most demanding cloud security standard, which sets a high bar for sovereignty, operational control, resilience, and trusted administration.

Bleu occupies a distinctive position within the European sovereignty landscape because it combines European governance and operational control with the technological maturity of a global cloud platform. It illustrates that sovereignty is not always achieved by replacing foreign technology, but can also be strengthened by redesigning where control resides within the stack.

This does not remove every dependency: the underlying cloud architecture remains based on American technology, and platform evolution continues to follow broader product development outside Europe. Yet for many regulated organisations, the decisive issue is whether critical control points – legal accountability, operational administration, data access, and governance – are sufficiently protected against unacceptable exposure.

In that sense, Bleu represents a pragmatic model of sovereignty-by-design: rather than absolute autonomy, it offers a structured balance between European control, regulatory assurance, and access to global cloud innovation.

EU-funded project for drone infrastructure surveillance

A consortium of more than 42 organisations, led by Nokia, has launched a major EU-funded initiative to develop advanced unmanned systems – airborne, surface and underwater – to monitor, protect and reinforce Europe's critical infrastructure. The project targets strategically sensitive assets such as energy grids, pipelines, rail networks, ports and subsea cables, reflecting growing concerns about sabotage, hybrid threats, and geopolitical vulnerability.

The consortium brings together startups, research institutes, and major industrial players, including NVIDIA, Safran, Leonardo and Saab. Together, they are developing autonomous vehicles equipped with advanced sensing technologies – such as laser systems, radar, and AI-driven perception – capable of operating in complex maritime and terrestrial environments and sharing data securely in real time.

This unmanned underwater vehicle is a Double Eagle from the Swedish defence company Saab and is used to detect and neutralise naval mines.

Running over a three-year period, the project exemplifies Europe's shift toward integrated, dual-use technologies that combine civilian infrastructure protection with military-grade capabilities.

Beyond its security objectives, the initiative is also expected to stimulate industrial growth, with projected revenues of around €90 million by 2035.[51] It illustrates how European industrial policy, technological sovereignty, and security concerns are increasingly converging around concrete, deployable systems rather than abstract strategy.

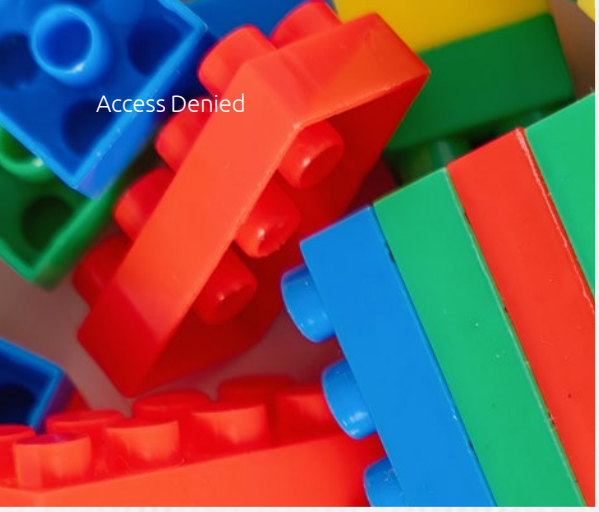
Gaia-X: from broad ambition to operational frameworks

Gaia-X was launched in 2019 as a European initiative aimed at strengthening trust, interoperability and transparency in cloud and data infrastructure. Its ambition was deliberately broad: to create a federated framework in which multiple providers could operate according to shared standards, while reflecting priorities such as privacy, portability, interoperability and data governance within European legal and economic contexts.

Rather than establishing a single hyperscale cloud provider, Gaia-X proposed an ecosystem of interoperable services connected through common rules, trust frameworks and certification principles. This gave the initiative a distinctive character: less focused on one provider, more on defining conditions under which data and cloud services could interact across organisational and sectoral boundaries.

The initiative quickly attracted wide attention. Numerous countries became involved, hundreds of organisations joined discussions, and Gaia-X emerged as an important reference point in Europe's debate on digital infrastructure. At the same time, its broad participation also introduced complexity. Governance structures became extensive, decision-making often required coordination across many actors, and the inclusion of global technology companies in working groups – intended to support interoperability and market relevance – prompted ongoing discussion about scope, balance and strategic positioning.

[51] Vifflin, N. (2025, June 4). *Nokia, Nvidia, defence firms back EU-funded drone infrastructure oversight project.* Reuters. https://www.reuters.com/business/aerospace-defense/nokia-nvidia-defence-firms-back-eu-funded-drone-infrastructure-oversight-project-2025-06-04/



For a period, Gaia-X was more visible as a framework under development than as immediately deployable infrastructure. Yet this also reflected the nature of the initiative: building shared standards and governance models across many sectors inevitably progressed differently from commercial cloud platform development.

Its longer-term significance lies increasingly in the practical instruments that have emerged around it: sector-specific data spaces, certification approaches and reference architectures in domains such as manufacturing, mobility, energy and healthcare.

In that sense, Gaia-X represents an important stage in Europe's digital development. It shows how broad values such as trust, interoperability and governance can gradually be translated into operational frameworks, even when implementation takes longer than initially expected.

Its eventual impact may therefore depend less on whether it becomes visible as a single infrastructure brand, and more on the extent to which its principles become embedded in how European data ecosystems are organised in practice over time.

French National Gendarmerie: long-term open-source transition creating some degree of sovereignty

While many public institutions continue to operate within long-established software ecosystems, the French National Gendarmerie adopted a different trajectory at an early stage. Beginning in 2005, the organisation gradually migrated parts of its IT environment toward open-source software, with Linux as a central foundation. What began partly as a cost-management initiative developed over time into a broader approach focused on operational control, lifecycle flexibility and long-term infrastructure consistency, resulting in some degree of sovereignty.

By reducing reliance on proprietary software in selected parts of its environment, the gendarmerie gained greater influence over update cycles, security configurations, system maintenance, deployment choices, and crucially, its data. Today, tens of thousands of workstations run on GendBuntu, a customised distribution based on Ubuntu, alongside open-source applications such as Firefox and LibreOffice. The environment is adapted to operational requirements and maintained within a framework designed to support continuity over time.

The practical effects have been significant. The transition has contributed to cost reductions, reduced certain forms of technical dependency, and increased operational resilience. Just as importantly, it illustrates that large public organisations can maintain extensive digital infrastructures using open-source components when long-term governance and internal expertise are aligned.

While the gendarmerie's experience does not suggest a universal model, it does show how specific architectural choices can gradually strengthen sovereignty without sacrificing convenience.

A clear pattern of practical digital sovereignty

Taken together, these examples reveal a clear pattern. Digital sovereignty is no longer pursued through grand, monolithic projects or abstract policy declarations alone, but through concrete architectural choices, targeted investments, and pragmatic alliances across the stack. Whether driven by startups, incumbents, public institutions, or governments, the common thread is a shift from passive consumption of global platforms to active stewardship of critical digital capabilities. Openness replaces opacity – not as ideology, but as a mechanism for trust and auditability. Control is redefined – not as isolation, but as the ability to decide *where* dependency is acceptable and *where* it is not. And scale is no longer the sole determinant of relevance; alignment of values, regulation, infrastructure, and execution increasingly is.

Instead of a single European model, we see a portfolio of approaches: open-source ecosystems alongside sovereign clouds; public-good AI next to venture-backed speed; national initiatives nested within European frameworks; small states leveraging unique assets; large institutions proving that autonomy is operationally viable. Together, they suggest that digital sovereignty is less a destination than a discipline – a continuous practice of design, governance, and investment. This also means that digital sovereignty should not be understood as a simple rejection of global technology providers. In many contexts, large hyperscalers such as Microsoft, Amazon Web Services and Google remain an essential part of the practical solution: they offer industrial scale, reliability, advanced services, and innovation capacity that many organisations cannot realistically replicate themselves.

The lesson is sobering but hopeful: sovereignty is unlikely to emerge through market forces or regulation alone. It develops incrementally, imperfectly, and often unevenly through accumulated design choices that translate ambition into durable digital capability.

Big Tech and the evolving meaning of sovereign cloud

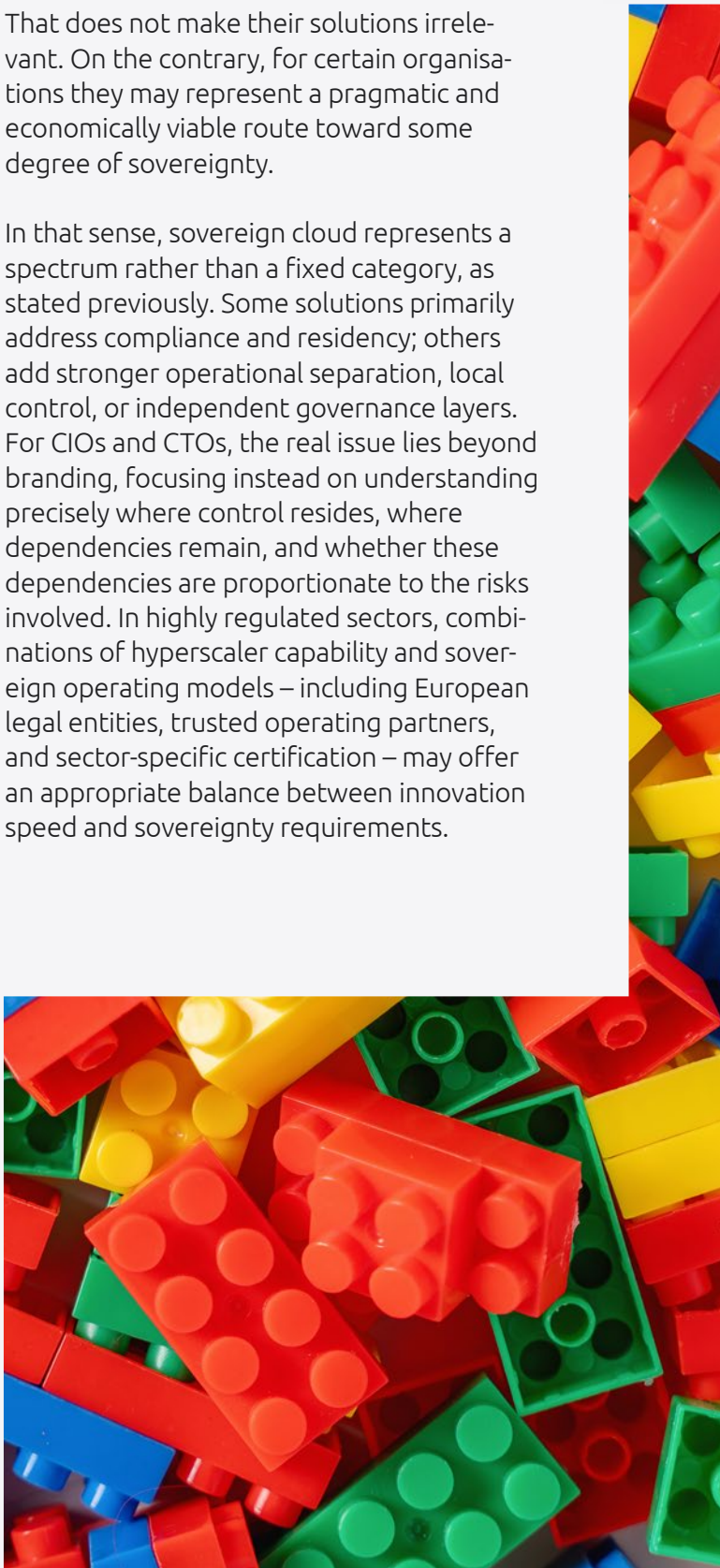
Europe's growing emphasis on digital sovereignty has also prompted a visible response from the large American hyperscalers. Companies such as Microsoft, Google and Amazon Web Services increasingly position parts of their cloud portfolio within European sovereignty requirements through offerings such as *EU Data Boundary, Sovereign Cloud*, and strategic partnerships with European actors.

In May 2025, for example, Google announced additional commitments for European customers, including regional data residency, governance measures under European legal frameworks, and an additional security layer under the name *Data Shield*, developed together with Thales.[52] Similar models are emerging elsewhere in Europe, often combining hyperscale infrastructure with local operational controls, legal safeguards, and sector-specific trust arrangements.

These developments matter because they show that sovereignty is increasingly being addressed within existing cloud ecosystems rather than outside them. At the same time, they also illustrate an important distinction: storing data in Europe or operating under European contractual arrangements does not automatically mean that every layer of technological control has shifted. Core infrastructure design, platform architecture, and product roadmaps often remain globally governed and hyperscalers remain under foreign jurisdiction.

That does not make their solutions irrelevant. On the contrary, for certain organisations they may represent a pragmatic and economically viable route toward some degree of sovereignty.

In that sense, sovereign cloud represents a spectrum rather than a fixed category, as stated previously. Some solutions primarily address compliance and residency; others add stronger operational separation, local control, or independent governance layers. For CIOs and CTOs, the real issue lies beyond branding, focusing instead on understanding precisely where control resides, where dependencies remain, and whether these dependencies are proportionate to the risks involved. In highly regulated sectors, combinations of hyperscaler capability and sovereign operating models – including European legal entities, trusted operating partners, and sector-specific certification – may offer an appropriate balance between innovation speed and sovereignty requirements.



[52] The Irish Times. (2025, May 21). *Google reassures EU cloud users amid concern over Trump threat.* https://www.irishtimes.com/business/2025/05/21/google-reassures-eu-cloud-users-amid-concern-over-trump-threat/

Conclusion

The building blocks of a more sovereign Europe differ widely in form, scale and maturity. Many remain relatively obscure, fragmented, or early-stage. Yet that is precisely where opportunity lies. For organisations seeking greater digital autonomy, familiarity supersedes grand declarations as the starting point for progress: understanding the emerging sovereign IT landscape, its actual capabilities, and its practical limitations. That understanding must be paired with a critical mindset. The growing political and commercial momentum around sovereignty has inevitably produced a broad spectrum of offerings that differ considerably in how deeply sovereignty is embedded. Some primarily address data residency and regulatory compliance, while others introduce stronger forms of operational separation, governance control, or strategic optionality.

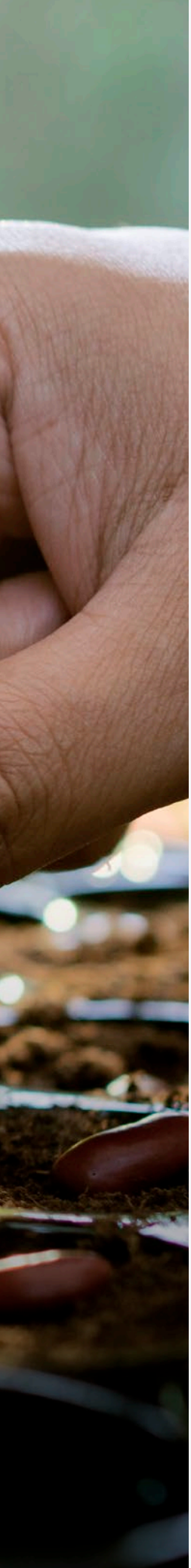
Distinguishing between these different levels of sovereignty maturity has therefore become a strategic competence in its own right: not every solution offers the same degree of control, and not every dependency is equally material.

The initiatives described in this chapter do not yet form a coherent system. But sovereignty has never been built in a single step. Their ultimate impact will depend less on individual success than on coordination, interoperability, and shared intent – across companies, sectors, and borders. Europe's challenges is not a lack of ingredients, but the discipline to assemble them into durable structures.

The case of Airbus, introduced at the start of the next chapter, illustrates this clearly. It shows how sovereignty is achieved through deliberate collaboration: aligning industrial capability, technological choice, and long-term strategy.

Chapter 5

The best time to plant a tree ...



Europe's current position in the digital landscape reflects a combination of historical investment choices, market dynamics, regulatory approaches, and the global evolution of technology ecosystems. Over the past decades, digital infrastructure, cloud platforms, and large-scale software ecosystems have developed unevenly across regions, often favouring environments where capital, scale, and coordination aligned early.

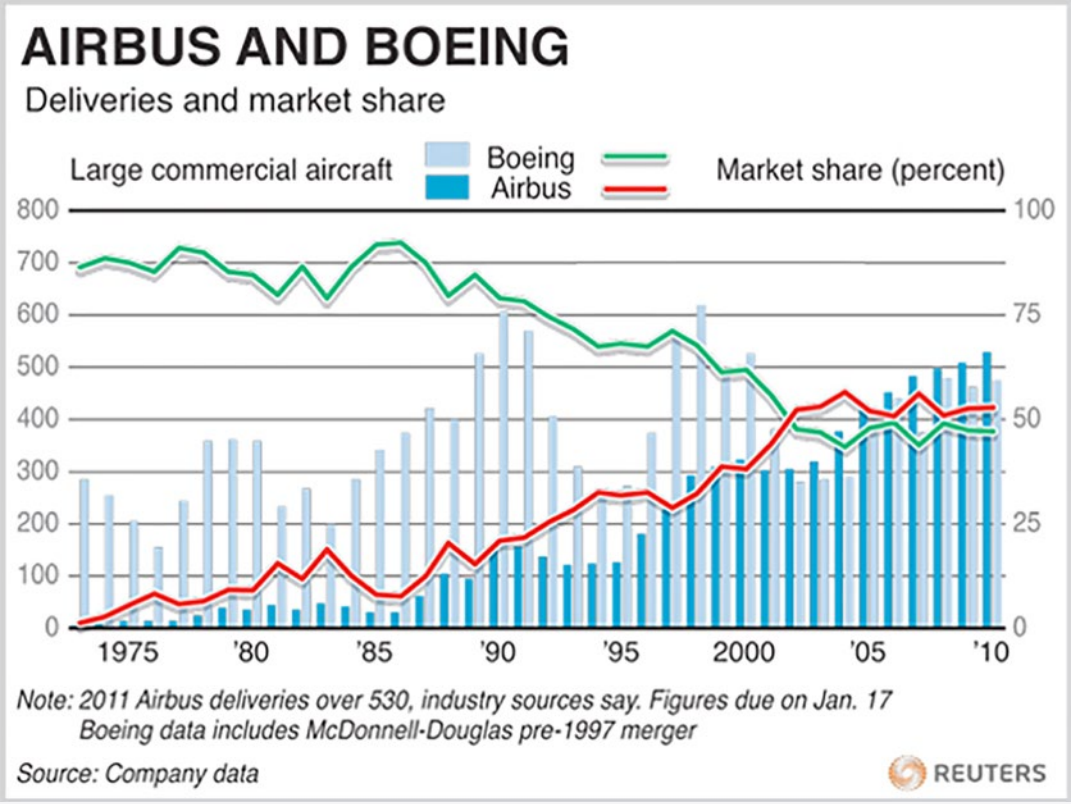
It is possible to consider alternative historical trajectories – scenarios in which Europe might have invested earlier or more extensively in digital infrastructure, software platforms, or startup ecosystems. The reality, however, is that there was simply insufficient interest at the time. Now, organisations and policymakers are increasingly evaluating where dependencies are acceptable, where diversification may be beneficial, and where additional capabilities are required to strengthen long-term optionality.

A well-known Chinese proverb captures the essence of this turning point:

The best time to plant a tree was twenty years ago. The second-best time is now.

In this context, the proverb reflects a practical observation: capability-building in complex systems takes time, and decisions made today will shape the range of available options in the future.

This chapter explores what it means to "plant that tree" in the present context – not as a symbolic gesture, but as a set of practical, incremental choices that may influence Europe's digital position over time.



Against all odds, a group of engineers in Europe in 1972 decided to set up a company to build passenger aircraft. Within forty years, they had grown to become the largest aircraft manufacturer in the world.

Airbus as a case study in long-term capability building

European history offers a powerful reminder that strategic autonomy can be built – if there is the will to do so. Airbus is a case in point.

In the 1960s, the global civil aviation market was largely dominated by US manufacturers such as Boeing and McDonnell Douglas. Several European governments identified aerospace as a strategically important sector and began exploring the feasibility of a jointly developed European aircraft manufacturer.

The initiative faced substantial challenges from the outset. It required coordination across multiple countries (France, Germany, Spain and the UK), alignment between political and industrial interests, and the development of complex engineering capabilities. Early programmes involved significant financial risk and long development timelines, and initial market adoption was gradual.

The first Airbus A300 aircraft entered service in the early 1970s, introducing design and efficiency characteristics that were competitive with existing alternatives. Over time, through continued investment, iterative development, and expanding industrial collaboration, Airbus evolved into a major global competitor. Today, Airbus and Boeing together define the structure of the commercial aircraft market.

The Airbus example is often referenced in discussions of strategic autonomy, but its relevance should be interpreted carefully. Digital infrastructure differs significantly from aerospace in terms of development cycles, capital intensity, network effects, and speed of innovation. However, the example does illustrate several broader points. Strategic capabilities can emerge over long time horizons through sustained coordination and investment, even when early phases are marked by inefficiencies, fragmentation, and uncertainty. Industrial scale and global competitiveness are rarely achieved immediately; rather, they develop gradually through persistence and iteration. In addition, collaboration across national and institutional boundaries can play a decisive role in building capabilities that would be difficult to achieve in isolation.

In this sense, Airbus is not a direct blueprint for digital sovereignty, but an example of how long-term capability-building can alter competitive positions under specific conditions.

Time horizons and trade-offs

One of the defining characteristics of digital capability-building is the tension between short-term incentives and long-term outcomes. In the short term, organisations often prioritise cost efficiency, speed of deployment, access to advanced features, and compatibility with existing ecosystems. These factors tend to favour large, established platforms that can deliver immediate value at scale.

Over longer time horizons, however, additional considerations become more visible. Dependency concentration may increase exposure to disruption or constraint, while switching costs can make it difficult to adapt when conditions change. Regulatory developments may introduce new requirements around data, security, or governance, and operational continuity may depend on factors that were not initially prioritised in architectural decisions.

Balancing these dimensions is inherently complex. Increasing control or diversification may introduce additional cost, integration effort, or operational overhead. Conversely, optimising for convenience and scale may increase reliance on a smaller number of providers. As a result, decisions about digital architecture are not binary choices. They are ongoing trade-offs between competing priorities.

Organisational implications: the CIO perspective

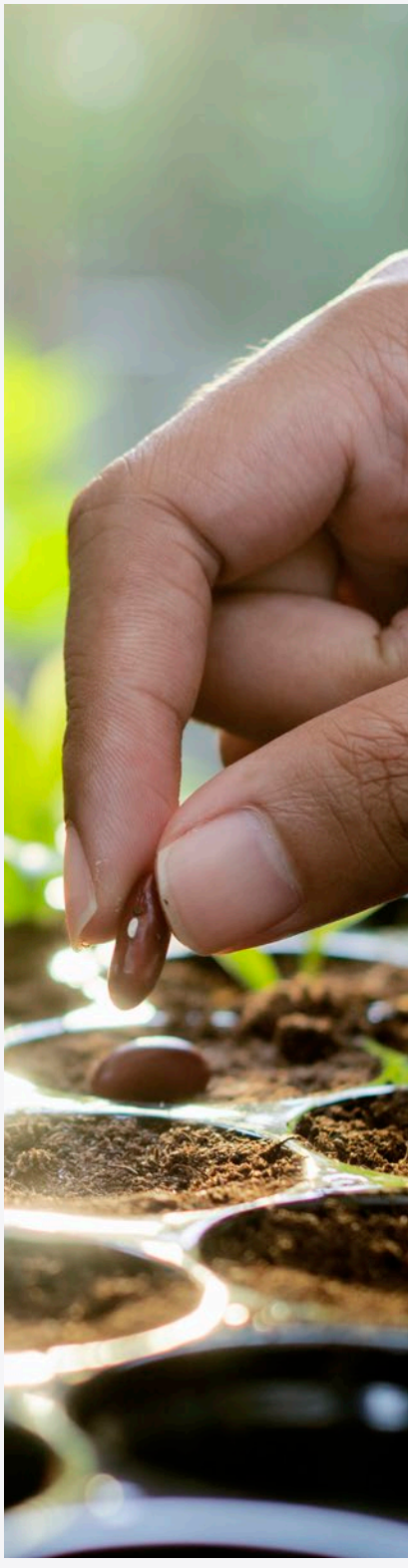
These dynamics have direct implications for CIOs and technology leaders. Rather than approaching sovereignty as an abstract concept, organisations benefit from analysing how dependencies manifest within their own environments.

At the system level, this involves understanding the extent to which critical workloads depend on specific platforms or providers, and whether alternative deployment options exist. Questions around portability, replication, and recoverability become central, particularly for systems that are essential to business continuity.

At the market level, attention shifts to vendor relationships and supply chains. Organisations assess how dependent they are on individual providers, whether credible alternatives exist, and how contractual arrangements affect flexibility over time. This includes examining exit conditions, interoperability, and the degree to which switching remains feasible in practice.

At the governance level, the focus turns to legal and operational control. This includes understanding which jurisdictions apply to data and infrastructure, whether systems can be audited or inspected, and how external policy or regulatory changes might affect access, usage, or continuity.

By analysing these dimensions in detail, organisations can move beyond general concerns about sovereignty and develop a more precise understanding of their exposure, resilience, and strategic options.



Incremental change rather than transformation

Experience across sectors suggests that changes in digital architecture rarely occur through large-scale, one-off transformations. Instead, they tend to emerge gradually through a series of smaller, cumulative decisions.

Organisations may begin by introducing alternative providers for specific workloads, particularly in areas where risk concentration is highest. Over time, they may adopt more interoperable architectures, making it easier to move data and applications between environments. Systems may be segmented based on criticality, with different approaches applied to core operations versus less sensitive functions.

At the same time, internal capabilities are strengthened, enabling organisations to exercise greater oversight and governance. Procurement criteria may evolve to include resilience, control, and long-term flexibility alongside cost and performance.

This incremental approach reflects both practical constraints and the complexity of existing systems. It also aligns with the broader observation that sovereignty, in practice, is not imposed through a single decision, but built over time through accumulated design and governance choices.

Looking forward

The question facing Europe – and organisations operating within it – is not whether to participate in global digital ecosystems. Such participation remains essential for innovation, competitiveness, and access to advanced capabilities. The more relevant question is how to engage with these ecosystems in a way that preserves sufficient flexibility, resilience, and control.

This requires a clear understanding of where dependencies exist and how critical they are. Some dependencies may be acceptable, particularly where alternatives would introduce disproportionate cost or complexity. Others may warrant diversification or additional safeguards, especially where they affect core operations or strategic assets.

In this context, technology decisions become closely linked to broader organisational objectives. Choices about infrastructure, platforms, and data are no longer purely technical; they are also strategic, affecting how organisations adapt to change, manage risk, and maintain operational continuity over time.

"Planting the tree," in this sense, is not a single act but a continuous process of evaluation, investment, and adjustment.

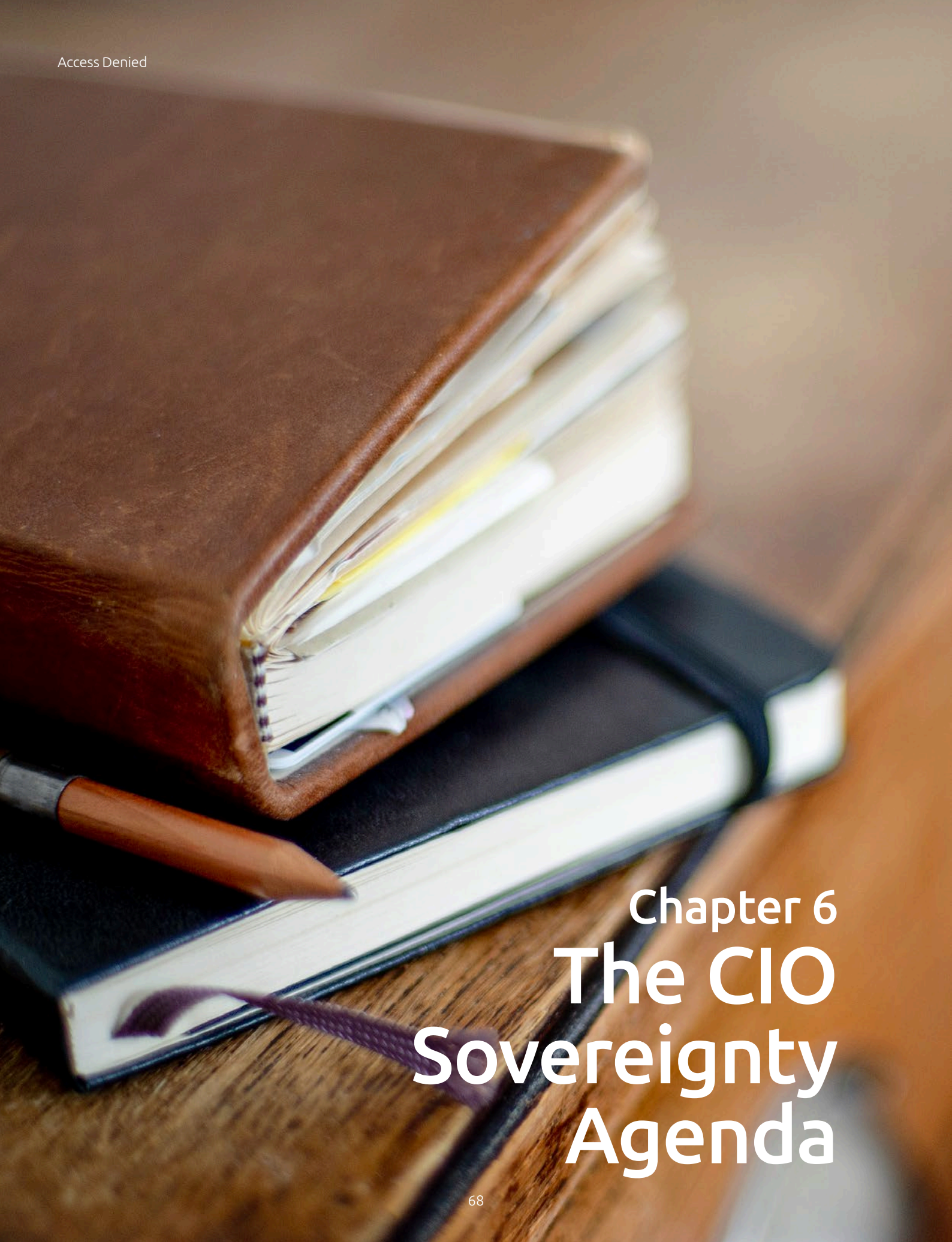
Conclusion

Europe's digital position today is the result of long-term structural developments rather than a single set of decisions. While past trajectories cannot be changed, future outcomes remain open and subject to ongoing choices.

The Airbus example illustrates that long-term capability-building can, under specific conditions, shift competitive positions over time. In the digital domain, similar outcomes – if they occur – are likely to emerge through a combination of incremental improvements, coordinated efforts, and sustained investment across multiple layers of the technology stack.

For CIOs and decision-makers, the implication is in most cases practical rather than ideological. Sovereignty is an ongoing set of decisions about architecture, governance, and risk management, made within a globally interconnected technology environment.

The next chapter examines how these considerations translate into concrete priorities for technology leadership.



Chapter 6
The CIO Sovereignty Agenda

Digital sovereignty is often discussed in the language of states – borders, jurisdictions, strategic autonomy. Yet sovereignty is exercised just as concretely inside organisations, in server configurations, architectural decisions, procurement policies and lines of code. Long before a geopolitical shock becomes visible in headlines, it is already latent in infrastructure. Europe's current position did not emerge from a single strategic misstep. It accumulated gradually, through thousands of rational decisions made in pursuit of efficiency, speed and scale. Cloud services were easier to adopt than to build. Platforms appeared neutral. Innovation felt frictionless. Over time, however, convenience hardened into dependency, and dependency introduces considerations around resilience and flexibility.

Recent industry research confirms that digital sovereignty awareness has now reached executive leadership. According to Gartner, 61% of Western European CIOs expect geopolitical factors to increase reliance on local or regional cloud providers, while more than 75% of enterprises outside the United States are expected to adopt a digital sovereignty strategy by 2030.[53] Sovereignty is no longer theoretical; it is entering procurement roadmaps. As one Gartner analyst summarised:

"Geopolitics is becoming a primary design constraint for enterprise IT."

For today's CIO, sovereignty is rapidly becoming an operational responsibility.

Digital infrastructure now determines who can act, who must comply, and who decides the boundaries of the possible. Systems may fail for technical reasons, but increasingly they are constrained by legal regimes, geopolitical pressure, commercial interests, and cultural assumptions embedded deep within technology stacks. The geopolitical dimension is no longer implicit. A recent Reuters report[54] described how governments are actively contesting data sovereignty policies internationally, with diplomatic pressure being applied to prevent localisation rules seen as threatening technological influence. Technology governance increasingly intersects with foreign policy and geopolitical negotiation.

---

[53] Gartner. (2025, November) 12. *Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers*. https://www.gartner.com/en/newsroom/press-releases/2025-11-12-gartner-survey-reveals-geopolitics-will-drive-61-percent-of-cios-and-information-technology-leaders-in-western-europe-to-increase-reliance-on-local-cloud-providers

[54] Satter, R. & Alper, A. (2026, February 25). *Exclusive: US orders diplomats to fight data sovereignty initiatives*. Reuters. https://www.reuters.com/sustainability/boards-policy-regulation/us-orders-diplomats-fight-data-sovereignty-initiatives-2026-02-25

The task confronting technology leadership is not to eliminate dependency – no organisation, and indeed no nation, can be fully self-sufficient. Even industry leaders acknowledge this reality. Capgemini CEO Aiman Ezzat recently noted that "*absolute sovereignty is unrealistic*", arguing instead for contextual autonomy across data, operations, regulation and technology layers.[55] The real question is subtler, and far more strategic: where is dependency acceptable, and where does it become existential?

Sovereignty, in practice, is the preservation of room to manoeuvre.
It is the ability to continue operating when conditions change.
It is the capacity to switch when switching becomes necessary.
It is, ultimately, the discipline of ensuring that critical choices remain available.

This interpretation increasingly aligns with global thinking on AI governance. Analysts now warn that by 2027, 35% of countries may become locked into region-specific AI platforms, driven by regulatory and geopolitical fragmentation.[56] Lock-in is no longer merely commercial, it is structural. What follows is an agenda – a way of seeing.

Five questions every CIO must now confront

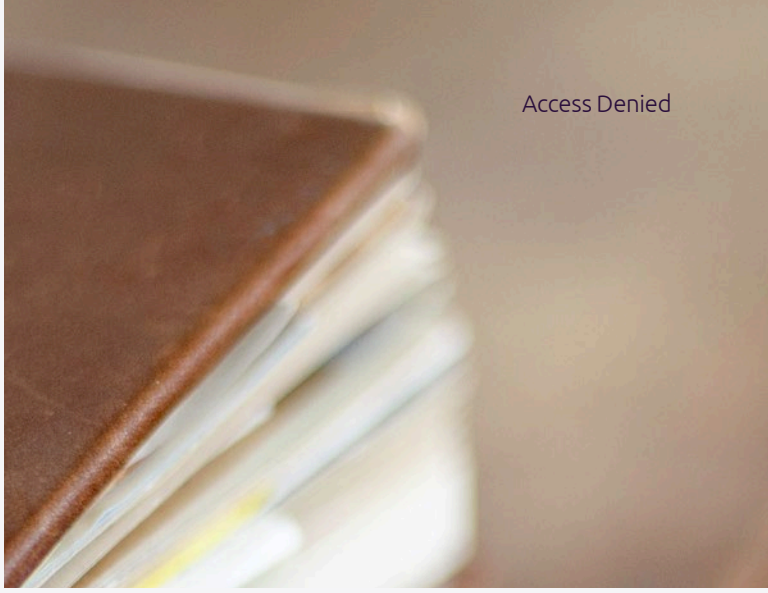
Moments of technological transition tend to obscure their own significance. Architectures evolve incrementally; dependencies deepen unnoticed. Only later does it become clear that what looked like a technical preference was in fact a strategic commitment. In this light, five questions increasingly distinguish organisations that actively shape their technology posture from those that rely more heavily on default platform choices.

1. Which digital capabilities are truly mission-critical to our autonomy?

Not every application carries the same strategic weight. Identity systems, data governance layers, and AI orchestration increasingly determine organisational continuity. European financial regulators have already warned that reliance on a small number of hyperscalers creates systemic risk across banking infrastructure.[57] The discipline lies in distinguishing convenience from necessity.

2. Where could dependency become strategically constraining?

Political decisions can restrict access to digital infrastructure just as effectively as technical malfunctions. What appears commercially stable may prove geopolitically contingent. Military leaders in Europe have recently warned[58] that attempts at rapid technological decoupling could themselves create operational vulnerabilities, precisely because critical systems already depend on foreign technology. The modern risk assessment must therefore extend beyond uptime and redundancy toward a more uncomforta-


Access Denied

ble question: under whose authority does this system ultimately operate? Dependency cuts both ways: interdependence pursued without architectural realism may introduce new fragilities.

3. Do we retain the ability to switch?

Lock-in increasingly has strategic as well as economic dimensions. Forrester analysts argue that complete disengagement from hyperscalers is unrealistic in the near term, recommending pragmatic sovereignty built through architectural flexibility rather than abrupt migration.[59] In addition to performance and costs, architectures should be evaluated on whether an organisation preserves the technical and operational latitude to change course. For sovereignty today is neither absolute nor binary. It is selective, layered, and contextual.

4. Which values are embedded in the technologies we deploy?

Digital systems may reflect assumptions about hierarchy, language, efficiency, risk and trust embedded in theur training data and design. As AI adoption accelerates, organisations increasingly inherit epistemologies alongside software. Industry observers now speak of "cognitive sovereignty", warning that AI systems trained elsewhere may subtly shape interpretation and decision-making itself. AI platforms are becoming not only operational infrastructure but interpretative infrastructure. When these systems are adopted, organisations do not merely outsource infrastructure, they import worldviews. Sovereignty is therefore not only about control over hardware and data, but about authorship of the technological environment in which decisions are made.

5. Are we optimising exclusively for efficiency, or also for long-term flexibility and resilience?

The most cost-effective architecture is rarely the most resilient. Sovereignty carries a financial, organisational, and sometimes cultural premium and introduces deliberate friction. PwC research[60] notes that emerging "sovereignty-by-design" cloud models are reshaping enterprise architecture precisely because compliance, resilience and geopolitical risk now coexist with innovation priorities. The question is not whether that premium exists, but whether leadership has consciously chosen how much vulnerability it is willing to exchange for convenience. The absence of an explicit trade-off is itself a decision.

---

[55] Marchandon, L. (2026, February 13). *Capgemini CEO dismisses calls for full European tech autonomy*. Reuters. https://www.reuters.com/business/retail-consumer/capgemini-ceo-dismisses-calls-full-european-tech-autonomy-2026-02-13

[56] Gartner. (2026, January 29). *Gartner Predicts 35% of Countries Will Be Locked Into Region-Specific AI Platforms by 2027*. https://www.gartner.com/en/newsroom/press-releases/2026-01-29-gartner-predicts-35-percent-of-countries-will-be-locked-into-region-specific-ai-platforms-by-2027

[57] Howcroft, E. (2026, February 3). *Europe must keep control of key technologies, says EU commissioner*. Reuters. https://www.reuters.com/business/finance/europe-must-keep-control-key-technologies-says-eu-commissioner-2026-02-03

[58] Financial Times. (2026, February 23). *Europe's 'tech sovereignty' ambitions carry security risks, military warns*. https://www.ft.com/content/0f7f7aa7-af4e-4ea6-82da-5f8c719982fe

[59] Bremmer, M. (2025, October 12). *Forrester: EU cloud sovereignty unrealistic for 2026*. CIO. https://www.cio.com/article/4070534/forrester-europes-cloud-sovereignty-remains-unrealistic-in-2026.html

[60] PwC in CIO. (2026, February 17). *Cloud Sovereignty: squaring compliance with innovation*. CIO. https://www.cio.com/article/4119786/cloud-sovereignty-squaring-compliance-with-innovation.html

A sovereignty risk scan

Dependencies seldom announce themselves dramatically. They accumulate quietly and surface abruptly, often in moments of stress or changing conditions. Legal exposure, operational concentration, supply-chain fragility and cognitive dependency increasingly overlap. AI accelerates this dynamic: dependency that once took decades to form may now emerge within a single product cycle. Global policy discussions reflect this shift. Also leaders at the World Economic Forum increasingly frame sovereignty as "strategic interdependence" – cooperation combined with selective control.[61]

The purpose of a sovereignty scan is clarity: only visible dependencies can be governed, only acknowledged constraints can be designed around.

Drawing the line: a decision matrix

Every organisation, implicitly or explicitly, draws a line between what it controls and what it entrusts to others. Sovereignty begins the moment that line is drawn deliberately.

A simple sovereignty decision matrix

The objective is deliberate control over those parts of an infrastructure where dependencies are deemed acceptable or unacceptable. In case of the later, trade-offs regarding costs, convenience and speed of innovation need to be reconsidered.

Technology layer	Accept dependency	Reduce dependency	Must control
Commodity SaaS	✓		
Collaboration tooling	✓		
Cloud infrastructure		✓	
Data platforms		✓	
AI models		✓	✓ (for critical domains)
Identity & access			✓
Encryption & keys			✓

Some technologies are interchangeable, commodity services whose replacement, while inconvenient, would not threaten organisational continuity. Others occupy a more ambiguous middle ground: cloud platforms, data environments, AI capabilities. Here the task is gradual risk reduction, preserving alternatives before they become urgent. And then there are foundational layers – identity, encryption, core data – where relinquishing control effectively means relinquishing agency. Seen in this way, sovereignty is less a destination than a pattern of choices:

- **Accept dependency where switching costs remain low.**
- **Reduce dependency where strategic leverage may emerge.**
- **Retain control where continuity depends on it.**

The precise boundary will differ across sectors. A hospital, an energy provider and a financial institution inhabit distinct risk landscapes. Yet the act of consciously defining that boundary is what transforms infrastructure into strategy.

[61] Davies, P. (2026, January 24). *AI sovereignty requires partnerships, not isolation, says World Economic Forum's AI chief.* Euronews. https://www.euronews.com/next/2026/01/24/ai-sovereignty-requires-partnerships-not-isolation-says-world-economic-forums-ai-chief

Architecture as an expression of sovereignty

In practice, sovereignty is architected patiently, often invisibly through design principles that privilege long-term flexibility and resilience over short-term optimisation. Academic research increasingly frames sovereignty as a first-class architectural quality attribute, comparable to security or reliability, requiring explicit design patterns rather than regulatory afterthoughts.[62] Replaceability becomes a strategic virtue. Systems need not be immediately interchangeable, but credible exit paths must exist. Without them, dependency quietly hardens into permanence.

Equally important is the separation of control from consumption. Organisations may rely on global platforms while retaining authority over identity, encryption, orchestration and data classification. These control layers form the true locus of sovereignty.

Interoperability, too, acquires new meaning. What once appeared as technical elegance now reveals itself as strategic optionality. Systems that cannot integrate are systems that cannot be escaped. Finally, data location emerges as more than a technical parameter. Data exerts jurisdictional gravity; where it resides, influences who governs it.

In this sense, architecture is never neutral. It shapes the range of future options available to the organisation.

Vendor posture in an age of geopolitics

Vendor selection increasingly involves considerations that extend beyond traditional procurement criteria, including legal, operational, and strategic factors. Technology companies themselves now acknowledge this reframing. Google has urged policymakers to pursue "open digital sovereignty", warning that excessive restriction could undermine innovation while recognising Europe's legitimate demand for control.[63] The decisive question now is whose technology it is, which values it embodies, and under what terms it operates. Those who write the software increasingly shape the worldview. Concentration can maximise efficiency and enable advanced capabilities at scale, while also introducing considerations around exposure and dependency that organisations may need to manage. Contracts, however meticulously drafted, do not supersede national law. Jurisdiction matters.

Distinguishing between transactional suppliers and strategic partners becomes essential. Some vendors provide tooling, others shape the environment in which the organisation itself must operate. The deeper a platform embeds itself into workflows, developer habits and data structures, the stronger its gravitational pull, and the narrower the exit. Vendor strategy now requires maintaining strong negotiating power in a market where technology and geopolitical influence intersect, moving far beyond traditional price-performance metrics.

AI and sovereignty at machinespeed

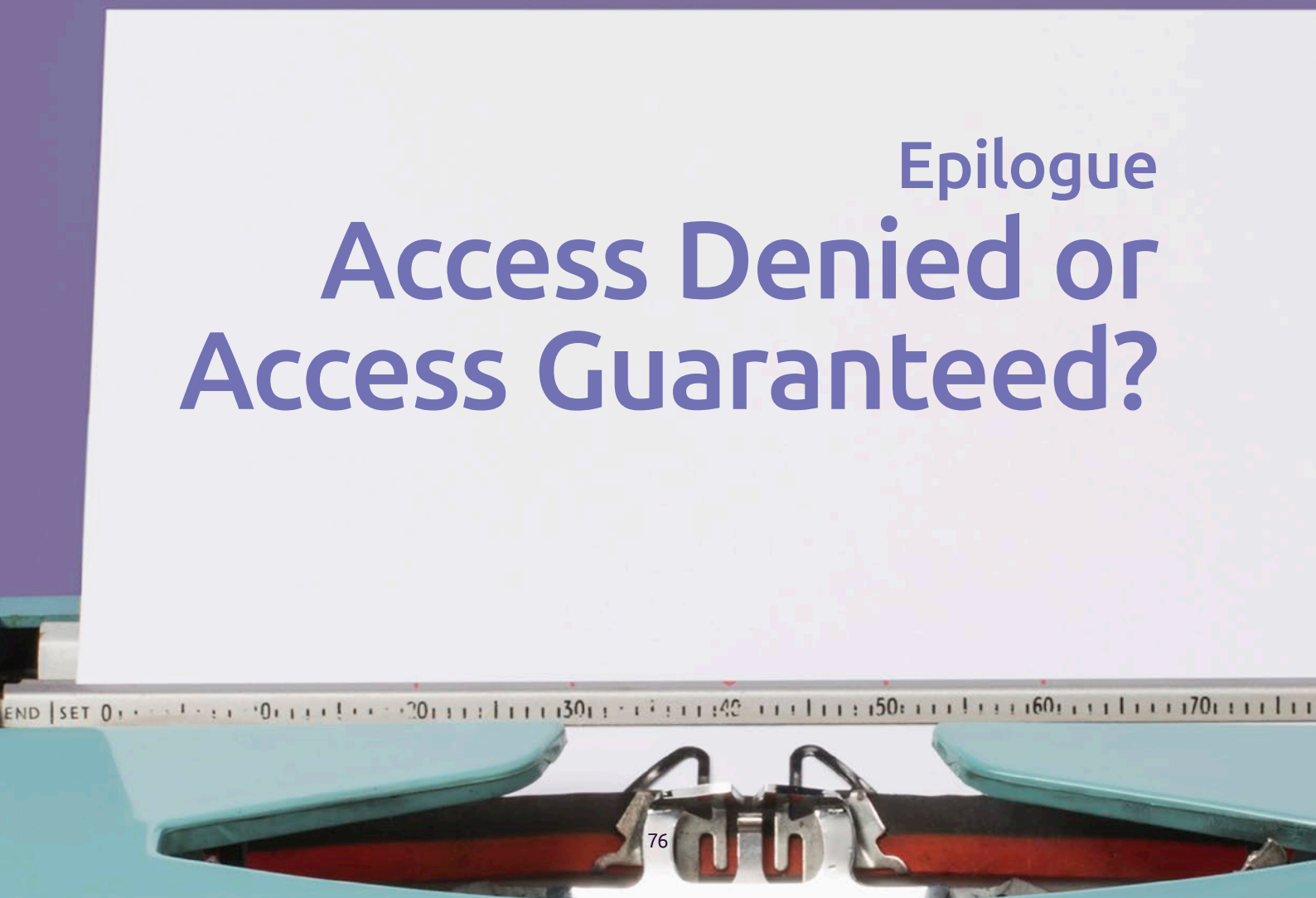
If cloud adoption unfolded over decades, AI is compressing dependency into years, perhaps even months. AI systems do more than process information: they reproduce the worlds on which they were trained. As such, they constitute not only technical infrastructure but cognitive infrastructure, quietly shaping how organisations interpret reality and make decisions. Here again, sovereignty does not demand total autonomy. Few organisations will build foundation models. Yet every organisation must decide where it positions itself along an emerging spectrum: consuming external intelligence, customising it, governing it, or in rare cases creating it. The risk lies less in choosing any particular position than in drifting into one unconsciously. As mentioned before, Gartner predicts rapid investment in domestic AI stacks as countries seek alignment with local laws, languages and cultural norms. Convenience accelerates lock-in. Opacity trades speed for control. The location and governance of training data can create structural advantages over time. To treat AI merely as another software category is therefore to underestimate its strategic weight.

From dependency to deliberate choice

Sovereignty is rarely lost in dramatic gestures. More often, it erodes through accumulated optimisations, each defensible in isolation. The responsibility now falling to CIOs is neither technological nationalism nor digital isolation. It is intentionality. Sovereignty does not require owning every layer of the stack. It requires ensuring that the layers defining organisational continuity remain governable, inspectable, and ultimately replaceable. For in the digital age, the most consequential forms of control are often invisible, exercised not through denial, but through defaults. Optionality is what separates dependence from strategy. And the organisations that preserve optionality today are the ones most likely to retain agency tomorrow.

[62] Esposito, M., Marchesi, L., Tonelli, R., & Lenarduzzi, V. (2026, February 5). *Sovereign-by-Design: A Reference Architecture for AI and Blockchain Enabled Systems*. https://arxiv.org/pdf/2602.05486

[63] Financial Times. (2026, February 12). *Google warns EU against 'erecting walls' in tech sovereignty push*. https://www.ft.com/content/0847914c-be27-4573-8600-8cdb54e604b7



Epilogue

Access Denied or Access Guaranteed?

From dependency to deliberate choice

While this report has largely been written from a European vantage point, reflecting its regulatory environment, market structure, and visible dependency patterns, the dynamics described are not uniquely European. They are structural features of a globally interconnected digital economy. Organisations in the United States, Asia, and elsewhere face similar questions around dependency, concentration, and control, even if expressed through different legal frameworks and market positions. Sovereignty, in this sense, is a shared challenge of navigating interdependence with clarity and intent.

Europe's current digital position is one expression of a broader pattern. It did not arise from a single decision, nor from a lack of talent or ambition. It emerged gradually, through thousands of rational choices made in pursuit of efficiency, speed, and scale. Cloud services were cheaper and faster. Platforms were easier to adopt than to build. Global standards felt neutral. Innovation appeared frictionless. Over time, these choices have increased reliance on certain platforms and ecosystems – patterns that can be observed across regions, even if their scale and direction differ.

What has become clear is that digital infrastructure is no longer just infrastructure. It increasingly shapes who can act, under which conditions, and within which legal, operational or commercial boundaries. Access to data, compute, software, and AI systems can now also be influenced by legal, regulatory, commercial, and operational factors embedded deep inside technology stacks. Many forms of influence in digital systems are embedded in standards, defaults, and accumulated dependencies rather than in explicit restrictions. These dynamics are not confined to any single jurisdiction. Even in markets where many of the dominant platforms originate, organisations operate within concentrated ecosystems that introduce their own forms of dependency, lock-in, and exposure to external change.

At the same time, the idea that technology is entirely neutral is increasingly being questioned. Digital systems encode assumptions about language, efficiency, hierarchy, risk, and trust. AI systems reproduce patterns present in the worlds on which they are trained. Platforms structure how people collaborate, communicate, and decide. When these systems are developed in different contexts, societies do not merely adopt infrastructure, they also adopt design choices, priorities and implicit operating assumptions. Sovereignty, in this sense, is about who can pull the plug and who shapes what becomes normal.

Yet the picture is not one of inevitability or decline. Across regions, additional approaches are emerging alongside global hyperscalers and established providers, often shaped by specific legal, operational and governance requirements. In Europe, this has taken a more visible form, but similar efforts can be observed elsewhere, reflecting a shared need to balance scale with control, and innovation with resilience. Fragmented, yes. Uneven in maturity, certainly. But increasingly relevant in specific contexts. What unites these efforts is not ideology, but a shared attempt to strengthen transparency over opacity, auditability over black boxes, interoperability over lock-in, and more deliberate long-term control over short-term convenience.

A crucial insight is that sovereignty in the digital age is not absolute. No country, organisation, or sector can be fully self-sufficient. The real question is where dependency is acceptable, and where it is not – requiring additional safeguards. Which systems are primarily convenient, and which are critical to continuity? Which layers must remain governable,

inspectable, and replaceable? Sovereignty today is selective, layered, and contextual. It is about preserving strategic freedom when conditions change.

Time plays a decisive role. Digital dependencies accumulate slowly, but they surface abruptly, often in moments of disruption. Encryption that feels secure today may fail tomorrow. Regulations that seem stable can be revised under pressure. Platforms that appear dependable may still be affected by changing legal, commercial or geopolitical circumstances. In this context, waiting for certainty is not neutral. Delay itself becomes a strategic choice, one that can narrow future options.

The most resilient response, therefore, is to design for flexibility and preserve optionality. That means building credible exit paths, testing migration feasibility, favouring open standards where appropriate, diversifying suppliers, and investing in capabilities that may appear inefficient in the short term but strengthen resilience over time. It also means recognising that sovereignty is built as much through trusted cooperation as through diversification. In many contexts, global technology providers remain an essential, and often irreplaceable part of the practical solution, providing scale, innovation, and reliability that few organisations can replicate. The challenge is conscious design of how these dependencies are governed, complemented, and made resilient over time, rather than total substitution.

The examples and arguments throughout this report are intended as illustrations of systemic dynamics, not as judgments on specific organisations, providers, or jurisdictions. The objective is to make visible the structural conditions under which digital systems operate.

History shows that Europe is capable of this kind of long-term commitment, when it chooses to think beyond immediate returns. Strategic autonomy has rarely been cheap, fast, or elegant. It has always required patience, political judgement, and a willingness to accept friction. The payoff usually comes later, often when the original scepticism has faded.

Ultimately, digital sovereignty is not a destination to be reached, nor a badge to be claimed. It is a continuous practice. It lives in architectural decisions, procurement choices, cultural awareness, and collective investment. It is strengthened through attention and eroded through habit. Lost quietly, rebuilt deliberately.

Europe cannot undo the path that led here – but neither can any region fully step outside the dependencies it has accumulated. What remains possible everywhere, is to shape how the next phase unfolds. The tools, talent, and ideas exist. What remains is the willingness to make deliberate choices – not perfectly, not uniformly, but with growing clarity about long-term consequences.

The best time to plant a tree was twenty years ago. The next best time is now.

What grows from that decision will determine whether future generations inherit a digital ecosystem they can help shape, or one whose terms are defined elsewhere.

Image credits

p. 14: DNB and AFM, in their report *Digitale afhankelijkheid in de financiële sector: risico's, weerbaarheid en Europese autonomie* (Digital dependence in the financial sector: risks, resilience and European autonomy, ed.). https://www.dnb.nl/algemeen-nieuws/persbericht-2025/afm-en-dnbwaarschuwen-voor-systeemrisico-s-financiele-sector-door-digitale-afhankelijkheid/

p. 18: Shoko Takayasu

p. 19: The Journal Investigates, source: European Commission. https://www.thejournal.ie/investigates-data-centres-6554698-Nov2024/

p. 24 left: https://en.wikipedia.org/wiki/Z3_(computer)#/media/File:Z3_Deutsches_Museum_b.jpg

p. 24 middle: https://upload.wikimedia.org/wikipedia/commons/4/4b/Colossus.jpg

p. 24 right: https://nl.wikipedia.org/wiki/ENIAC#/media/Bestand:Glen_Beck_and_Betty_Snyder_program_the_ENIAC_in_building_328_at_the_Ballistic_Research_Laboratory.jpg

p. 32: Data Center Watch. (2025). $64 billion of data center projects have been blocked or delayed amid local opposition. https://www.datacenterwatch.org/report

p. 44: https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-aeuropean-alternative-for-digital-sovereignty

p. 45: https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-aeuropean-alternative-for-digital-sovereignty

p. 57: https://www.saab.com/products/double-eagle

About the authors

Menno van Doorn
is the director of SogetiLabs' Research Institute. His accolades include being christened the 'IT researcher of the year' by *Computable*, a distinguished IT magazine. Van Doorn's academic pursuits are deeply rooted in behavioural economics and the science of advertising.

Sander Duivestein
is a keynote speaker, trend analyst, internet entrepreneur and strategy consultant on the impact of digital technology on people, companies, and our society. He is also a frequent guest on various radio and television programmes.

Thijs Pepping
is a humanist and techno-philosopher. He researches how digital technology reshapes our humanity and develops the concept of the Digital Art of Living, a way of life for the algorithmic age. He writes, teaches, and gives keynotes on the ethical and existential impact of emerging technologies.

About VINT labs.sogeti.com
VINT, the Sogeti research institute and part of SogetiLabs, provides a meaningful interpretation of the connection between business processes and new developments. In every VINT publication, a balance is struck between factual description and the intended utilisation. VINT uses this approach to inspire organisations to consider and use new technology. VINT research is done under the auspices of the Commission of Recommendation, consisting of • K. Smaling, Chief Technology Officer Continental Europe Aegon (chairman) • J. Behrens, Vice President and General Manager Google Maps Automotive • M. Boreel, Chief Technology Officer Sogeti Group • M. van den Brink, Head of Sogeti Netherlands • P. Dirix, Chief Executive Officer Port of Moerdijk • L. Holierhoek, interim COO/ CCO Holwater BV • D. Kamst, Founder and Chief Executive Officer Klooker and Smyle • M. Krom, Independent Executive Digital and IT Consultant • T. van der Linden, Group Information Officer Achmea • Prof. dr. ir. R. Maes, Professor of Information & Communication Management Academy for I & M • P. Morley, Lecturer Computer Science University of Applied Science Leiden • E. Schuchmann, Ministry of the Interior and Kingdom Relations • M. Smeets, CIO DELTA Fiber Nederland BV • R. Visser, CIO NN Group

Special thanks to the *comité scientifique* for their contributions.

About SogetiLabs
SogetiLabs is a community of over 150 technology leaders from Sogeti worldwide. SogetiLabs covers a wide range of digital technology expertise: from embedded software, cybersecurity, deep learning, simulation, and cloud to business information management, IoT, mobile apps, analytics, testing, and blockchain technologies. Visit labs.sogeti.com

About Sogeti
Part of the Capgemini Group, Sogeti makes business value through technology for organizations that need to implement innovation at speed and want a local partner with global scale. With a hands-on culture and close proximity to its clients, Sogeti implements solutions that will help organizations work faster, better, and smarter. By combining its agility and speed of implementation through a DevOps approach, Sogeti delivers innovative solutions in quality engineering, cloud and application development, all driven by AI, data and automation.
Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion. Visit www.sogeti.com

sogeti labs
Part of Capgemini

FSC

Printed on FSC-Certified paper.

Sogeti Global Marketing Ref. 00681 April 2026.