

TECHNOLOGY

The big debate: has digital sovereignty gone too far?

Is digital sovereignty crucial for businesses to succeed in the AI era or is it merely thinly veiled anti-Americanism? Two experts have their say

Tamlin Magee

18 Aug 2025



Digital sovereignty is a term on the lips of every tech leader. Loosely defined, it refers to organisations' control over their own tech stacks in accordance with domestic regulations. In a digitally sovereign territory, neither software nor data is subject to extraterritorial laws, such as the [US Cloud Act](#), which stipulates that any US business must surrender data to US intelligence agencies should they demand it.

Although the concept is not a new, digital sovereignty has grown in popularity across Europe, particularly since the start of [Donald Trump's second presidency](#). JD Vance's 'Munich' speech at the start of this year, in which the US vice-president seemed to decry political currents across Europe, alerted many on the Continent to the increasingly cosy [relationship between Silicon Valley's tech firms and the US administration](#).

Technologists and politicians once viewed seamless digital borders as essential to the global data economy. With data and AI increasingly viewed as crucial security concerns, however, ramparts have emerged along national borders.

But the movement, if it can be called that, is polarising. Advocates are keen to [promote domestic alternatives](#) to 'big tech' providers, arguing that smaller countries are being bullied by Silicon Valley firms and the US government. Opponents, however, say the internet must remain borderless; that there should be more, not less, collaboration across national borders. Here, two experts in the field share their views.

It is not possible to build a valuable stack without internationalism



Amanda Brock
CEO of OpenUK

Twenty years ago, with the emergence of cloud computing, the first rumblings of sovereignty and protectionism emerged. Around that time, I asked a service provider where their "European server" was located. Nobody had asked them that before. The answer? Texas. Clearly, citizen data and privacy had to be better protected and governments did step in to ensure more robust protections.

Nearly all services depend on digital technology, so countries that rely on technology infrastructure or services of companies based in other jurisdictions are vulnerable. Such dependencies cannot sensibly be ignored. Resilient national infrastructure is a must. Risk must be mitigated, but the key question is, "How?"

The term 'digital sovereignty' is often muddled and inconsistently applied, meaning discussions of how to achieve it occur at cross purposes. The definition ranges from hosting and managing a stack locally to excluding US software entirely.



Every country should seek the best innovation for its citizens

Small, domestic players, particularly in the EU, have seized an economic opportunity for preferential treatment with both hands. Their enthusiasm for sovereignty is not entirely altruistic: they'll benefit from increased revenue streams, so it's unsurprising that they encourage nations to exclude international tech. Yet, for all this talk of sovereignty, countries still use US-made chips – [even China](#).

If we're honest, much of the aggression directed at the US in this context is thanks to the success of its tech sector. Criticisms are often intertwined with anti-big-tech sentiment. Unsurprisingly, the US administration has come out fighting. These sovereignty-based attacks have directly contributed to the Trump [administration's tariffs](#).

Every country should seek the best innovation for its citizens. And that is accessed through global collaboration. [Tech stacks must be open and visible](#) to diminish dependencies on particular suppliers. Almost all (96%) commercial software is somewhat dependent on open-source technology, which is based on international contributions that have long tails of dependencies on other code. It is impossible to build a valuable stack today without internationalism.

Governments should focus on opening technology up instead of policing where it's from. Building a software stack from scratch requires open-source technology, which is built by a collaborative, global community. If technology is transparent, we can iterate and innovate on top of it.

The term 'sovereignty' is being weaponised, and excluding US tech will not benefit the EU. The UK's Compute Road Map balances investment in the long-term future of the domestic tech sector with international collaboration. It aims both to protect both UK population and the domestic economy and to ensure UK citizens have access to the best-possible digital services. The technologies supporting these services can be localised as appropriate to build a sovereign suite.

Sovereignty around AI and data is existential



Kevin Dallas
CEO, EnterpriseDB

Applications are rapidly integrating all four types of artificial intelligence: predictive, generative,  entic and, soon, physical. But there's no AI without data. If you don't provide the right data,

algorithms can hallucinate and deliver false insights. Control over AI systems, as well as the data those systems use, is therefore an existential concern.

What does this mean? If companies are to benefit from AI tools, they must control the data that feeds those tools and be the ones to decide how and where AI is deployed. And the government in their jurisdiction must control the security, compliance and regulatory requirements of the AI used within their boundaries.

We asked 2,000 C-suite executives about digital sovereignty. Most said it is a strategic matter, not a political one. About nine in 10 (92%) believe digital sovereignty will drive the operational resilience and AI performance they need. Only 8% are motivated by geopolitics to pursue digital sovereignty. Firms cannot afford to leak data to third-party large language models.

Nine in 10 C-suite executives believe digital sovereignty will drive the operational resilience they need

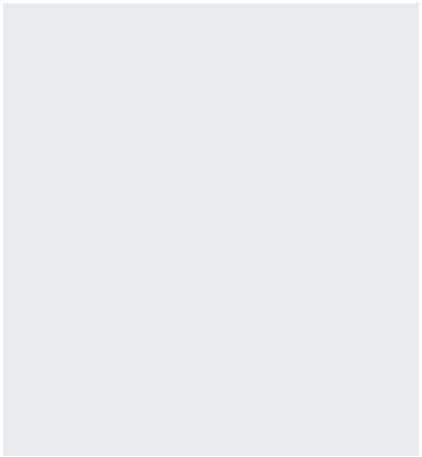
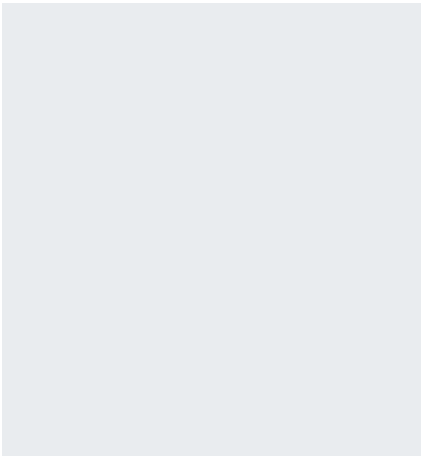
One only has to look at AI's contribution to global GDP, forecast by PwC to be \$16tn (£12tn) to 2030, to understand why companies and governments are seeking to secure an adequate share of this GDP growth. This is why countries such as Germany, the UK, China and the US are starting to consider what [new compute infrastructure is needed for artificial intelligence](#) and how to put it together.

They're asking: Where do these compute resources get deployed? Is it in-country or in-region or global? What security are you going to provide around that data? What compliance requirements does your industry have? What regulatory requirements does your nation have? That's the changing landscape.

Sovereign AI is a national agenda item for China, the UK, Germany, Saudi Arabia, the UAE, India and so on. These countries realise that they need AI sovereignty to be globally competitive. There's also a huge appetite for investors and enterprise CEOs to embrace sovereignty and control their future with a sovereign-data-layer platform.

GLOBAL BUSINESS / RISK & REGULATION / TECHNOLOGY / ARTIFICIAL INTELLIGENCE / CLOUD
COMPUTING / RISK

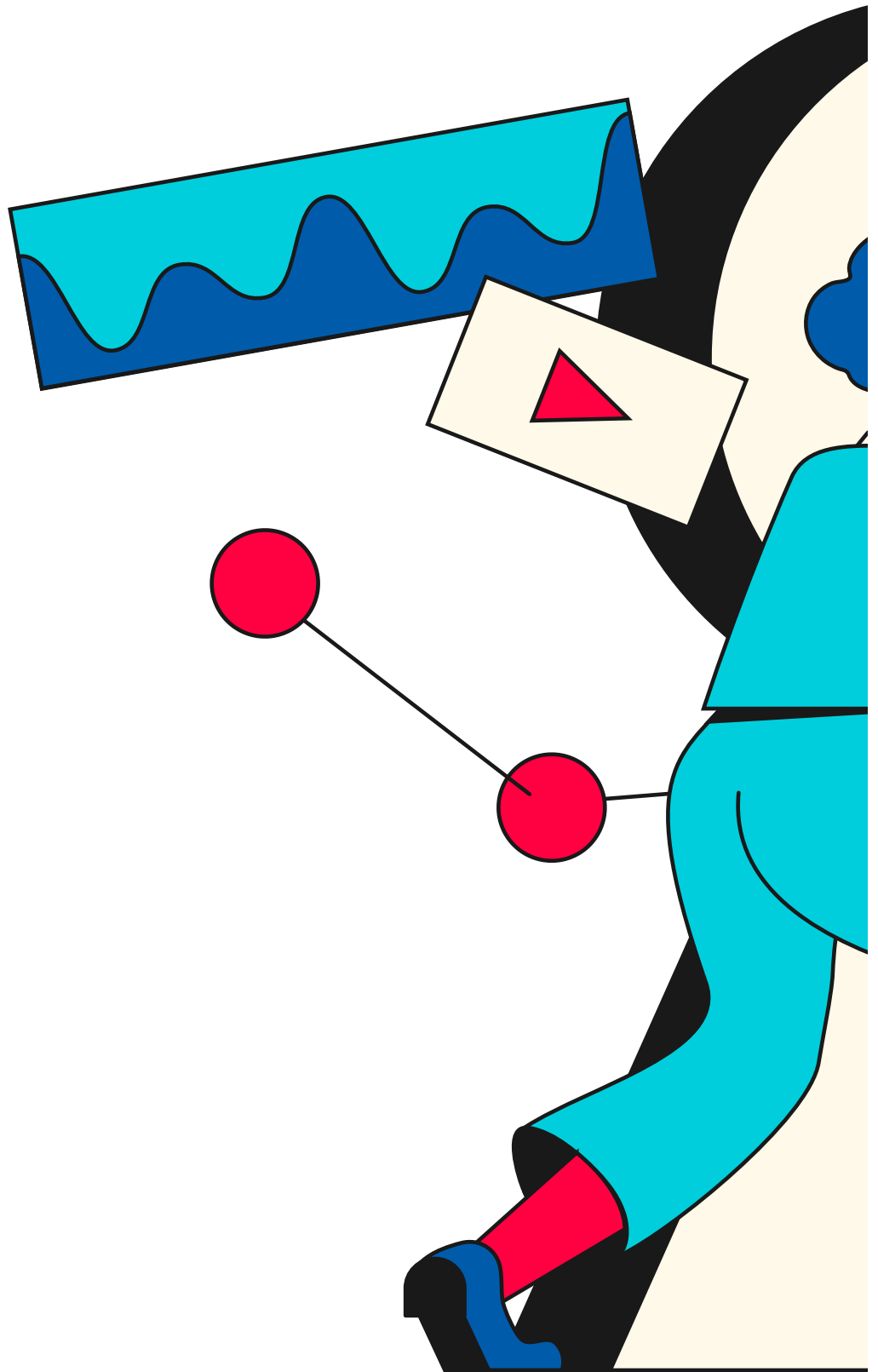




READ THIS NEXT

RESPONSIBLE BUSINESS	FUTURE OF WORK	FINANCE & INVESTMENT	TALENT & CULTURE	RISK & REGULATION	TECHNOLOGY
Dancing with calipers: Lush’s CEO on the messy reality of leading with values	Poor tech access bars children from learning digital skills	New fraud law puts whistleblowing to the ultimate test	Three-minute explainer on... quiet cutting	Security experts weigh in on UK’s proposed VPN crackdown	Chatbot ‘wellness’ obscures grotesque ethical violations of AI industry





Subscribe to our Daily Newsletter

Receive the latest insights direct to your inbox, and gain access to our extended article t

Your email address



RELATED ARTICLES

FINANCE & INVESTMENT

The ONS has been miscalculating the UK’s gender pay gap for 20 years: is it still fit for business?

FINANCE & INVESTMENT

Could failing your financial goals boost your stock price?

FINANCE & INVESTMENT

Meet the new hedge fund bankrolling AI data centres

OPINION

The surprising realisation when I trained an AI to write like me

SUBSCRIBE

Your email address

SUBSCRIBE

- About us

Contact us

Write for us

Work for us
- Advertise with us

Partner with us

- Privacy Policy

Terms & Conditions

We use cookies and other data collection technologies to provide the best experience for our customers. You may request that your data not be shared with third parties here: [Do Not Sell My Data](#).



