WORK AND DIGITALISATION 17.11.2025 | Leevi Saari

The big tech playbook

By framing digital sovereignty around regulation and political autonomy, big tech has deflected attention from deeper critiques of its systemic power

The second reign of Donald Trump has spurred an unprecedented merging of tech and state power in the United States. The administration has proven vindictive in its punishments, and transactional and prodigal in doling out its patronage. By catering to the whims of the president, Silicon Valley companies hope to secure export licenses, avoid competition-policy inquiries, acquire lucrative state contracts and streamline permitting for data centres. While tech and power have always been close, funding of presidential ballrooms and televised pledging of fealty to the president signal a change in the historical juncture.

This increasing alignment comes with a cost. By becoming entangled with the Trump administration, tech companies become parties to the geopolitical dramas of the day. The administration has shown a willingness to use coercion to achieve geopolitical aims, with trade deals driven by force and American companies used as extensions of sovereign power. As a consequence, trading partners are looking for alternatives, with calls for 'digital sovereignty' trending internationally.

The digital sovereignty conference this week in Berlin has to be understood against this background. The geopolitical *raison d'état* is challenging the long-standing dominance US tech giants have enjoyed in Europe. Even if European politicians hesitate, the vain hope is that courts will eventually force their hand by banning the use of certain US products.

Such aspirations are not lost on US hyperscalers (the dominant global cloud providers). In fact, they have already adapted by redefining strategic narratives, developing new compliance products and collaborating with European companies.

Varieties of digital sovereignty

Digital sovereignty is an elusive concept. Instead of trying to nail down 'what it *is*', one useful way to grapple with it is to ask: what do we need digital sovereignty *for*?

In debates on digital sovereignty, three rationales are typically woven together: we need it for *regulatory autonomy* (to enforce rules and protect rights), for our *political autonomy* (to prevent being cut off or coerced), or for reasons of *economic autonomy* (to capture value built on top of digital technologies).

From the perspective of an American company, these three are hierarchical in terms of importance: the first you can commercialise, the second you can de-risk, but the third is existential. Hence, the objective is to keep the debate as much as possible in the world of rules and regulations.

This argument might seem counterintuitive. Indeed, the European legislative machinery and its regulatory prowess are often seen as the bulwark against tech power. But despite the very tangible costs and challenges, this is a ground on which hyperscalers are comfortable. As long as they can keep the discussion at the level of regulatory autonomy, the costs are manageable. Companies can append new technical, legal and operational tools. The resulting product is then sold back to the sovereignty-minded consumer under the guise of enhanced security protections. This 'productisation' effectively neuters geopolitical pressure and can even become a source of further advantage by raising standards to a level that crowds out competitors.

In an unexpected turn of events, this sovereignty debate has become a site for competition-by-proxy between American hyperscalers.

The political autonomy argument is trickier, but not existential from a corporate perspective. It can be de-risked with technical and legal innovations. Last spring, Microsoft unleashed a new flurry of European 'sovereignty commitments', ranging from solemn promises to use legal means to challenge Trumpian carnage, to a fully European board, to storing copies of source code in vaults in Switzerland.

Recent trends also include bringing new coalitions of interests to the fray. This includes partnerships with local 'partner clouds' where, in exchange for a share of rents, a local company provides plausible deniability and a sovereignty buffer that insulates hyperscalers from political attention. For example, Microsoft partnered with SAP's subsidiary Delos Cloud to

deliver a 'sovereign' version of MS Office to the German government with an up to 20 per cent mark-up. In an unexpected turn of events, this sovereignty debate has become a site for competition-by-proxy between American hyperscalers. Alphabet, the parent company of Google, recently noted that European digital sovereignty is best served by breaking Microsoft's vendor lock-in in the productivity software markets.

Now, whether hyperscalers can truly provide credible assurances to Europe is up for debate. In a French Senate hearing, a Microsoft representative admitted under oath that US law ultimately prevails. The idea that Europe can gain full control is largely an illusion, since the rules are often built into the infrastructure itself. Will the European 'continuation partners' truly make the trek over the snowy Alpine peaks to recover copies of Microsoft's source code? And could such code even be used when disconnected from the company's update cycles?

This is a field in which the hyperscalers enjoy a structural advantage. Microsoft employs over 1 600 CELA (Corporate, External and Legal Affairs) professionals and legions of engineers, and it is in the process of building data centres across Europe to close the window for data-localisation-based obstacles to business. The longer technocratic debates over data protection, compliance playbooks and other standards drag on, the higher the barriers become for the less fine-grained but more foolishly hopeful task of imagining truly different technological paths.

Paths forward

The European Commission and the European Data Protection Supervisor recently blessed the use of MS Office in EU institutions after new data protection measures. Competitors are already noting the possibility that new environmental standards will be unattainable by others. Debates on digital sovereignty are currently trending toward definitions that would exclude considerations of ownership or the geographic location of the ultimate owner, opening the field for hyperscalers' sovereignty playbook.

Why does this narrowing succeed? The easy answer would point to typical stories of 'big tech lobbying'. However, there are structural questions as well. The structurally imbalanced transatlantic relation, now etched in humiliating trade deals, has limited the policy space in the European Union. Sparking the anger of Trump is a real risk to car manufacturers, pharmaceuticals and industrial manufacturers. In this hard bind, it is tempting for policy-makers to replay the playbook of the early 2000s: to engage in a therapeutic and nostalgic call for data protection, compliance and security till your ears bleed, speaking of

international partnerships and trusted partners, and praying that Newsom will prevail in 2028 and bring us back to the natural order of things.

Substituting the questions on digital sovereignty for increasingly complex legal and procedural rules might backfire by erecting a compliance wall that only big tech can scale.

But blaming politicians is also a form of therapeutic talk and an intellectually dishonest one at that. Political will alone doesn't create infrastructure. Concrete actors need to put money on the table, and we must wrangle out of the convenience of building 'light' applications on top of 'heavy' infrastructure. Reproducing a part of the capex bill of building data centre infrastructure is a task that challenges conventional MBA management philosophies. For even the largest European tech companies, wanting to keep margins and balance sheets clean, it is tempting to partner with hyperscalers to create the 'best quality for the customers'. While rational for an individual company, this strategy splits the front of 'European tech' as a coherent countervailing power that would start redirecting money flows to alternative technological infrastructures.

Paths forward are not easy. Attempting to wholesale replace the planet-spanning compute infrastructure would be unrealistic. However, while for some use-cases this computation capacity is a necessary feature, for most cases, dependence on hyperscalers is driven not by need but by convenience. Profit-driven companies are an awkward fit as midwives to strategic technological development, and the Trumpian grip over Europe cannot simply be wished away on the grounds of it being humiliating, inconvenient or plainly unpleasant.

But a path needs to be charted nonetheless. Substituting the questions on digital sovereignty for increasingly complex legal and procedural rules might backfire by erecting a compliance wall that only big tech can scale. Instead, engineers, politicians, dreamers and technologists need to face the material challenges of crafting an alternative technology future. This requires business courage and shrewdness, skills that have withered under the weight of legalistic governance.

It requires doing away with the outdated dogmas of liberalism-vs-protectionism or open-vs-closed-source as the constitutive conflicts of technology politics, thinking instead about other binaries, such as hype-vs-real and useful-vs-useless innovation. It requires targeting resources,

building with purpose and prioritising with taste.

And maybe, somewhere hidden under the veil of elliptic curves, such a European alternative is gestating, where technological dreams beyond MS Teams are forged anew.



Leevi Saari

Leevi Saari works as EU Policy Fellow at the AI Now Institute and as Researcher at the University of Amsterdam.