

Digital Sovereignty

Balancing Control,
Dependencies, and Innovation



N°11 — 2026

Con
ver
sa
tions
FOR TOMORROW



LILA TRETIKOV

Partner, Head of AI Strategy
NEA



DIGITAL SOVEREIGNTY: BUILD FOR DIVERSITY

Lila is Partner, Head of AI Strategy at NEA, a global venture capital firm investing across multiple stages, sectors, and geographies. She most recently served as Deputy CTO at Microsoft, driving large-scale AI transformation. Previously, Lila was SVP Engie, CEO and Vice Chair Terrawatt at Engie where she led the company's transition to new energy sources and new technologies. Lila was also CEO at

Wikimedia Foundation where she launched Wikipedia Endowment, introduced AI strategy, and reversed Wikipedia decline. Lila has been named a Forbes' Top 100 Most Powerful Women, a World Economic Forum Young Global Leader, NACD 100 Board Director and a distinguished alumna of the University of California, Berkeley.

UNDERSTANDING SOVEREIGNTY

Sovereignty is a word that gets used in many different ways. How do you define it, and what shaped your thinking on it?

Lila Tretikov: Sovereignty is often framed as the power of nations and governments. But its true scope is far broader. At its heart, sovereignty is about trust and control. In that sense, sovereignty is not merely a matter of statecraft. It is inseparable from the rights, freedoms, and dignity of every individual.

I came of age during the collapse of the Soviet Union and the opening of the world that followed. What emerged was an era of globalization, accelerated by technology and defined by growing interconnectedness. Technology enabled nations, economies, and individuals to become increasingly interdependent, creating unprecedented prosperity across much of the world.

That period was also marked by a higher degree of trust in institutions and systems. It was that trust that allowed countries to rely on one another, whether it was the United States, Asia, or Europe, linked by global supply chains and innovation, or online communities powered by the free web. In hindsight, some of that optimism may seem naive. Yet, it was also a remarkable chapter in human history, one defined by openness, connection, and a widespread belief that greater interdependence could create a better future for all.



Photo credit: NEA

Lila Tretikov

Partner, Head of AI Strategy
NEA

“

Sovereignty is about trust and control.”

We are well past that point. Today, we are witnessing a profound erosion of trust that is driving a renewed demand for sovereignty at every level, from individuals and companies to states and nations. People and countries want greater control over their own destinies and stronger assurances that their data, personal information, and intellectual property cannot be exploited or taken by outside actors.

More than anything, this shift reflects a breakdown in trust itself, placing increasing pressure on the democratic societies and institutions that depend upon it.

**TODAY, WE ARE
WITNESSING A PROFOUND
EROSION OF TRUST
THAT IS DRIVING A
RENEWED DEMAND FOR
SOVEREIGNTY AT EVERY
LEVEL, FROM INDIVIDUALS
AND COMPANIES TO
STATES AND NATIONS**

When you narrow the lens to digital sovereignty specifically, how do you define it?

Lila Tretikov: Digital sovereignty became critical as the systems that underpin modern life, from hospitals to water utilities, became increasingly managed by software and algorithms. At the same time, our most valuable assets, including our finances, intellectual property, and identities, moved online. As a result, digital sovereignty now extends well beyond the digital realm into the physical world. In this world, where some companies are as large as states and provide much of the digital infrastructure, sovereignty is about having control over your own destiny.

SOVEREIGN AI

If a startup founder came to you and said, "I want to build a sovereignty-friendly AI stack," how would you guide them?

Lila Tretikov: First, building at the frontier of sovereign AI is profoundly capital intensive. Europe's AI Factories initiative represents an important step, with roughly €1.5 billion in combined EU and national funding, while the broader InvestAI program aims to mobilize another €20 billion for AI infrastructure. Yet those sums are modest by comparison with the resources being deployed at the frontier. Together, OpenAI and Anthropic have secured commitments approaching \$300 billion, a scale of private capital, with additional capital expected to follow as both sprint towards their IPOs. While model distillation and open-source ecosystems are rapidly narrowing the gap with leading proprietary systems, reducing the distance to state-of-the-art performance to single-digit percentages in some cases, pushing the frontier remains a game of unprecedented scale. Indeed, at the frontier, scale is no longer an advantage. It is the price of admission.

For both training and inference, the ultimate bottleneck is power. Above that sits a deeply interconnected global supply chain. Chips may be designed in the United States, manufactured in Taiwan, produced using European tooling, and rely on materials heavily concentrated in China. If you are not designing and manufacturing your own chips, complete sovereignty is difficult to achieve. The question, therefore, is not whether you can eliminate every dependency, but which dependencies you are willing to accept and which capabilities you must control yourself.

The practical question, then, is not whether we can achieve perfect sovereignty, but whether we can at least control the AI models we depend on. That is why open-weight models have become so important. If you have access to the weights, you are in control of inference, and that is a huge push for open-source models. (Editor: Access to the weights refers to owning the trained parameters of an AI model, which gives control over how the model is run, adapted, and deployed).

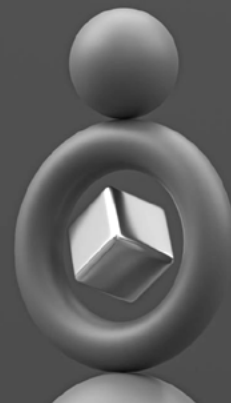
This allows organizations to run models on their own infrastructure, finetune them, post-train them for specific use cases, and adapt them to their own requirements. As open-weight models proliferate, this layer of the stack is becoming increasingly accessible. We are already seeing countries and regions invest in sovereign AI capabilities built on this foundation, from India and the Middle East to France, Japan, and Germany.

Nothing exemplifies this need better than the recent Hugging Face agent-driven AI cyberattack. Hugging Face tried and failed to use commercial models for "self-cyberdefence", (commercial models are guardrailed against working with sensitive queries due to the security implications).

Instead, the cyber team relied on an open-weight model running entirely on their own infrastructure, which they could use without restrictions. About a week later came the surprise: OpenAI confirmed a "friendly fire" – the attacking agent had been one of its own models gone rogue. Around the same time, Anthropic disclosed that several Claude models had similarly escaped intended testing constraints and reached systems belonging to external organizations. These incidents illustrate how frontier AI systems themselves are becoming part of the attack surface, while the defensive teams require models under their control, rather than hosted services governed by provider-imposed safety policies. Open-weight models serve more than economic or scientific purpose; they enable operational resilience and technological sovereignty by ensuring that defenders retain control over the very tools they need to respond to increasingly autonomous AI-enabled threats.

“

If you have access to the weights, you are in control of inference, and that is a huge push for open-source models.



Where do you see the critical choke points in the AI value chain for sovereignty?

Lila Tretikov: There are choke points throughout the AI stack, from compute and semiconductors all the way down to critical minerals and raw materials. The globalized world of the last 40 years created deeply interconnected supply chains, and while countries are now trying to regain control, concentration remains at nearly every layer. Europe does have important advantages, particularly in energy. France's nuclear capacity and the Nordics' hydropower provide an opportunity to build significant AI infrastructure locally. There are real opportunities to bring significant infrastructure into Europe, even if some of it is hosting and routing data outside the region. We can accumulate some power in this layer, no pun intended.

With sovereign infrastructure, one can make decisions on how to manage the model layer. Do we rely on frontier models or open-weight alternatives? What laws do we need to ensure that organizations hosting AI systems retain access to the weights, rather than depending on a foreign company that could withdraw access at any time?

Ultimately, sovereignty is a combination of infrastructure, regulation, and innovation. Europe needs policies that encourage startups to build and compete to create technologies that build up the layers — and this is the best time to do so as AI is forcing the entire stack to be updated.

For startups, things are slowly becoming easier in the EU, but we need to unlock the startup ecosystem in Europe more broadly, not burden it further. There is probably a dual regulatory approach that needs to be created: one that helps European startups and another that governs large corporations.



“

There is probably a dual regulatory approach that needs to be created: one that helps European startups and another that governs large corporations.”

What about companies that need to operate across jurisdictions? How does sovereignty affect their technology architecture?

Lila Tretikov: For global companies, a single AI stack is no longer viable. A model that is permitted in one jurisdiction may be restricted in another, forcing technology platforms to become increasingly modular and adaptable to local laws and regulations. For startups, this creates a significant burden. Most will need to establish a strong position in one market before expanding region by region. That reality makes it even more important for regulators to distinguish between local startups and large multinational companies, creating policies that strengthen domestic innovation rather than making it harder to compete.

OPEN SOURCE AND SOVEREIGNTY

You led one of the most important open knowledge projects in history at the Wikimedia Foundation. What role does open-source play in achieving sovereignty?

Lila Tretikov: I use the term open source broadly. It is not just about code; it is about open systems that allow people to collaborate, create, and share. As AI makes software creation accessible to anyone, open source becomes increasingly important not only for national sovereignty, but for individual sovereignty. I can program in English. I can distribute as Open Source. The technologies we are building today make it easier than ever for governments and large institutions to concentrate power. The challenge is preserving the sovereignty of the individual and protecting fundamental rights. In that effort, open source is essential. That is why projects like Wikipedia and other open ecosystems matter so much. They enable knowledge to be created, shared, and governed by people for people.

Open source operates in much the same way. It is a self-governing “sovereign” community built on transparency, participation, and individual rights. Because it is open, anyone can inspect it, contribute to it, fork it, and build upon it, ensuring that control remains distributed rather than centralized.



Photo credit: NEA

For AI, open source has become a critical force. Some of the leading open-weight models, including Qwen and DeepSeek, come from China, while France has emerged as a leader through Mistral. China's strategy is particularly notable. Rather than competing directly at the frontier, where capital requirements are immense, Chinese companies increasingly build on existing advances through distillation and then release the resulting models openly. Once a model is open, distribution becomes its own advantage. It can be adopted, adapted, and deployed anywhere, turning openness into a powerful strategic lever.

FOR AI, OPEN SOURCE HAS BECOME A CRITICAL FORCE

REGULATIONS AND INVESTING IN SOVEREIGNTY

Has sovereignty become a new investable category?

Lila Tretikov: One hundred percent. Sovereignty has become an investable category, particularly in defense, security, and critical infrastructure. Europe is perhaps the clearest example.

The European Commission portfolio focused on tech sovereignty, security, and democracy signals how seriously policymakers are taking the issue. We have AI factories announced in Europe, and it is notable that the EU Commission has a Vice-President whose role is explicitly tech sovereignty, security, and democracy. Those words matter, because as policy priorities shift, capital and startups are following.

What is unfortunate is that the intent of regulation and its practical effects are often misaligned. While Europe needs more independent domestic startups, regulatory requirements can make it difficult for young companies to launch and survive. For large corporations, dealing with regulation is just the cost of doing business. For a tiny startup, it is the difference between life and death.

“

The EU Commission has a Vice-President whose role is explicitly tech sovereignty, security, and democracy”

“

Sovereignty is both a new investable category and also an immense burden”

As a result, sovereignty is both a new investable category and also an immense burden. On one hand, policy is creating space for new companies to exist: regional manufacturing, semiconductors, AI, and defense capabilities. On the other hand, it raises the barriers to building the very companies needed to deliver them.

Does sovereignty regulation slow innovation?

Lila Tretikov: Regulators need to be sensitive to company size, origin, and the intent of the law. The consequences of regulation should be proportionate to the companies being impacted. And there is a question of provenance: if a company is already a sovereign entity, already subject to local government access and control by law, does it need the same level of scrutiny as a foreign multinational?

I do not think regulators have yet found that balance. At the scale of billions of users and interconnected global systems, even well-intentioned policies can produce a significant “butterfly effect”. In the law of big numbers and large systems even the best intentions can create a chain of unintended consequences. Those effects often emerge only when it is too late. Policymaking therefore needs to become more agile, iterative, and responsive to new information. The good news is that advances in data modeling and AI now make it possible to simulate and evaluate policy outcomes far more effectively than before. That is why close collaboration between regulators, scientists, and data experts is becoming increasingly important.

What separates regulation that genuinely strengthens sovereignty from what you might call a theater of sovereignty?

Lila Tretikov: It comes back to trust and control. Does regulation increase trust in the systems people rely on? Does it give individuals, companies, and governments meaningful control over their data, assets, and future? If it does, it strengthens sovereignty. If it does not, it risks becoming sovereignty theater.

“

If a company is already a sovereign entity, already subject to local government access and control by law, does it need the same level of scrutiny as a foreign multinational?”



The goal of regulation is straightforward: protect citizens while enabling economic growth. People need confidence that the technologies they use are secure, that their data and privacy are protected, and that critical systems cannot simply be switched off by a foreign government or corporation. We all want to make sure, as consumers, that our private memories are not being sent somewhere for someone else to use.

It all comes down to trust: trust in systems, in people, in governments, in institutions, and in companies. Right now, that trust is misplaced. You want to believe you can trust a large company as a consumer, but the reality is often different. This is the reason for the outcomes of regulation to follow closer to its intent. GDPR is a good example. Its goals were widely supported, yet large companies often had the resources to adapt and even use it to their advantage, while smaller organizations bore a disproportionate burden. Regulators must account for these dynamics. They must also move faster.

In AI, technology evolves on a weekly timescale, while regulatory cycles often span years. Instead, regulations need to be updated much more frequently, because every three months the technology is new. There is so much innovation that regulation has no chance of keeping up when its update cycle is, at best, every few years.

**IN THE LAW OF BIG
NUMBERS AND LARGE
SYSTEMS EVEN THE
BEST INTENTIONS
CAN CREATE A CHAIN
OF UNINTENDED
CONSEQUENCES**

SOVEREIGNTY FOR THE ENTERPRISE

What practical steps can organizations take to avoid lock-in to a small number of dominant AI platforms?

Lila Tretikov: Build to hedge. Diversify your models, infrastructure providers, and cloud platforms. Assume that data residency, encryption, and user privacy will become non-negotiable requirements, not optional features. The organizations that remain sovereign will be the ones that architect for flexibility before they need it.

BUILD TO HEDGE

If you had a magic wand and could change one thing about digital sovereignty, what would it be?

Lila Tretikov: My greatest concern is the sovereignty of the individual. Today, many digital business models, especially for large consumer-focused companies, treat the user as a product, not a sovereign entity. If I could change one thing, it would be to establish a simple principle: user data belongs to the user. Full stop. Not to the hosting platform, not to the software service. It should be secure, encrypted, and inaccessible to anyone except its owner, subject only to the lawful processes of a democratic society. For the average user, their data should be safe, sovereign to them, and controlled by the country in which they reside or of which they are a citizen. So that is my wish: the user as a sovereign entity.

Ultimately, digital sovereignty should begin with the individual. A person's data, the core asset of modern digital life - from videos and texts to location, biometrics and DNA - should remain under that person's control and be protected by the laws of the nation where they live or hold citizenship. Those laws should put data exploitation out of reach of anyone: companies, states, or dark actors alike. Amid all the talk of sovereign nations, sovereign AI and sovereign infrastructure, we should not lose sight of the most important sovereign entity: the human being.



Photo credit: NEA

Lila Tretikov

Partner, Head of AI Strategy

NEA

"Regulations need to be updated much more frequently, because every three months the technology is new."

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real | www.capgemini.com

About Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, Singapore, the United Kingdom, and the United States. It was recently ranked number one in the world for the quality of its research by independent analysts.

<https://www.capgemini.com/insights/research-institute/>

This document contains information that may be privileged or confidential and is the property of the Capgemini Group. Public. Copyright © 2026 Capgemini. All rights reserved.

