Tech Sovereignty and Data Governance: Policy Paper

This year will be one of the most significant in terms of global digital governance.

The World Summit on the Information Society (WSIS) is undergoing its 20-year review; a new UN 'Global Digital Compact' has been agreed that gives nation states and the UN greater say in digital governance; and the role of multinational 'Big Tech' firms is increasingly viewed via the lens of politics and diplomacy.

At the core of these issues is tech sovereignty. Countries are increasingly trying to steer conversations around digital transformation that will affect their citizens — all while seeking to capitalize on technology to boost local economies and improve overall competitiveness.

To address how tech sovereignty interlinks with questions about data governance and global trade, the Geneva Graduate Institute, Caribou Digital and the Atlantic Council's Democracy and Tech Initiative held a seminar on March 24 to unpick the varying definitions of tech sovereignty. The seminar also focused on how countries, citizens and industry are navigating an increasingly geopolitical world surrounding how data is collected, stored and used globally.

As part of the discussion, participants focused on three core conclusions:

1) The digital sphere has become inherently geopolitical — made up of both nation states and global tech companies with citizens caught in the middle.

2) There is a lack of definitions for key concepts like tech sovereignty, data sovereignty and cyber sovereignty and how they apply to different policy areas from trade to internet governance.

3) Countries want to increase their sovereignty and control over data, but this must be done in a collaborative and multi-stakeholder approach to uphold a free and interoperable internet.

Geopolitics of digital

The seminar made clear that technical concepts like tech sovereignty and data governance were no longer merely technical or legal issues. They are geopolitical ones. Data, in particular, has become a crucial asset for both governments and technology companies — its use fundamental to fuel everything from global trade relations to the latest artificial intelligence models.

This shift has only become stronger in early 2025 where a change in US political leadership, a faltering global economy and increased hostility between long-time

international allies have positioned technology at the center of many of these geopolitical debates.

What had been, until recently, bureaucratic or business decisions around the location of data centers, the investment in high performance computing infrastructure, and the signing of bilateral agreements on the free flow of data have now become tense political decisions taken by countries' most senior leaders, as well as bargaining points in global trade relations.

For Global Majority countries, policymakers are trying to carve out appropriate domestic policymaking space to develop their domestic tech sectors, including the adoption of digital industrial policies that touch on issues around tech sovereignty and data governance.

For Global North countries, there is increased digital trade-related tensions between the United States, China and the European Union that have extended into policy decisions around semiconductor manufacturing, data flows, AI and quantum computing.

For citizens of all countries, these shifts have left many disconnected. Tech sovereignty, in its widest definition, is not just about states. It's also about self-determination at all levels of society, and the current politicization of the digital realm has left people being acted upon — and not being asked to participate — by both state and industrial actors that view their role as mostly passive in how these concepts are developed and implemented.

A Lack of Definitions

The seminar highlighted a basic difficulty when discussing tech sovereignty. There is no clear, single definition.

Participants discussed concepts like "digital sovereignty," "cyber sovereignty," "AI sovereignty," as well as other technical areas like "data localization," "data governance," and "data sovereignty." They acknowledged many of these terms are used interchangeably yet mean different things, and that has led to confusion among policymakers about how they can be implemented.

In the trade sector, for instance, concepts like data sovereignty are currently viewed as a restrictive tool that harms global trade as it limits how data can be transferred across borders and leads to regulatory fragmentation.

In the digital sector, however, some countries are pursuing policies that impose greater government control on citizens' data — potentially via data localization policies that require such information to be stored within national borders. This is viewed as a necessary step to ensure greater control over how that data is used, but can be perceived as either an overreach by governments that harms citizens' rights or a threat to the existing global trading order.

A fundamental initial step in these ongoing conversations is to define what “sovereignty” means within the digital realm, especially given the fact that , politicians and policymakers will continue to talk over each other and will not be able to communicate nor align on a common step of principles.

So far, China is the only country to articulate a clear vision for “tech sovereignty” in a way that places the state at the center of digital policymaking. That stands in tension with democratic traditions of a multistakeholder approach to internet governance and without further work may challenge the dominant vision of an open and interoperable internet.

What is needed from democratic countries, was a clear narrative about what the pillars and principles of tech sovereignty should be to maintain the existing digital system that has created decades of global economic benefit and promoted human rights in an increasingly digital world.

Sovereignty and Control, but Make it Open

The seminar concluded with a discussion about countries’ efforts to exert more control of concepts of tech sovereignty and data governance. As mentioned above, national senior leaders are now at the center of these debates, and many are trying to impose greater checks on a digital world that is inherently borderless, bottom-up and fast-moving.

That urge will not go away. But participants stressed the need to reframe government efforts to “own” the digital sphere. Instead, some suggested the concept of self-determination — at both a national and citizen level – could be a productive way to answer many of the questions that were posed during the seminar.

At its core, “tech sovereignty” is about self-determination, or the ability for lawmakers, officials and even individuals to express their own will on complex digital systems. Where the balance of power lies amongst these will determine who shapes our digital future. Many participants stressed that such decisions should include sovereign people, and must include the ability for individuals to exert their own control over industry services that can place people out of reach of the true ownership of their data.

That incorporates the idea of autonomy without being exclusionary — a key principle to open`` an interoperable internet governance model.

For countries, the need to impose greater control over technology, especially via data and internet governance structures, was repeated several times during the seminar. Participants, however, expressed a willingness to collaborate and cooperate internationally on implementing such greater control. The goal, based on the discussion, was to develop on existing global governance models to provide national politicians and officials a greater ability to both define what needed to be done and then facilitate bilateral and multilateral cooperation to effect change for national citizens.