Couture, Stéphane, Sophie Toupin, and Christoph Borbach, 2025. "Sovereign AI, the fragmented internet, data crawlers, and the opacity of consent forms: A dialogue on digital sovereignty." *communication +1*, vol. 11, issue 2, pp. 1—19.
DOI: https://doi.org/10.7275/cpo.3555

Sovereign AI, the fragmented internet, data crawlers, and the opacity of consent forms: A dialogue on digital sovereignty

Stéphane Couture, Université de Montréal, CA, stephane.couture@umontreal.ca
Sophie Toupin, Université Laval, CA, sophie.toupin@com.ulaval.ca
Christoph Borbach, University of Siegen, GER, christoph.borbach@uni-siegen.de

In this dialogue with Stéphane Couture and Sophie Toupin, the discursive point of departure is their canonical paper from 2019 on the various notions of sovereignty when referring to the digital—and what has changed since its publication in discursive, legal, and technological dimensions. In the conversation, Couture and Toupin trace the term's evolution across activist, Indigenous, and state contexts, showing how it functions as a boundary object—a concept that travels between domains, is used by different communities and groups, while holding a stable identity. At stake here are issues of sovereign AI, the fragmentation of the internet, data crawlers as part of extractive generative AI, and the opacity of consent forms. Couture and Toupin emphasize design, infrastructure, and consent as crucial terrains where sovereignty is materially negotiated and constructed. Reflecting on digital resistance, Toupin and Couture argue that practiced digital sovereignty represents a conceptual shift from reactive defiance to proactive reappropriation: an affirmative politics of infrastructural self-determination. The dialogue revisits Indigenous and Global South perspectives, stressing digital sovereignty as a decolonial struggle for epistemic and material autonomy. Finally, Couture and Toupin question the anthropocentrism of sovereignty discourse, proposing a Latourian posthumanist understanding that remains attentive to ecological entanglements, opening up the imagination of a sovereign Earth as a provocative space for reflection.

*

Christoph: Your paper "What does the notion of 'sovereignty' mean when referring to the digital?"[1] has already joined the canonical literature in the discourse on issues of digital sovereignty. What were your motivations and background for writing the paper? What was the central finding of the study?

Sophie: Our article began with a question. A friend and activist-scholar had edited a non-academic special issue on technological sovereignty. We asked ourselves: Why was our friend suddenly using the term *sovereignty* to describe what she and her community were doing? Why was an activist who had spoken for years of autonomy, now turning instead to the language of sovereignty? What was happening in this shift? It was over lunch with Stéphane at a neighborhood coffee shop that we decided to write about this.

Stéphane had long been reflecting on questions of state sovereignty and the digital through the lens of Free, Libre and Open Source Software (FLOSS) and he was commissioned by the Quebec government to conduct a study on the topic during his postdoc at McGill University. I was a PhD student at McGill University at the time, and had been involved for a few years with tech activists in Montréal and beyond. Our initial motivation for this article was straightforward: We noticed that the tech and digital activist community around us had begun using a term that surprised us, and we set out to explore what *sovereignty* means for them in a digital context. As we started our literature review, we quickly realized that a wide range of actors—including Indigenous peoples, feminists, and states among others—were invoking the term *sovereignty* in relation to the digital. Our goal was simple: to help ourselves, as both activists and scholars, better grasp what was unfolding at the discursive level. At the time of writing, we never anticipated that the article would be widely read.

Looking back, we can better understand what was happening at the level of the conjuncture. In 2012 in Canada (also known as a part of Turtle Island), Idle No More—a movement launched by four Indigenous women—swept across the country in response to a bill introduced by Stephen Harper's Conservative government that threatened Indigenous rights to clean water, land, and food. The movement's website declared: "Idle No More calls on all people to join in a peaceful revolution to honour Indigenous sovereignty and to protect the land & water & sky." While Idle No More did not explicitly invoke the notion of digital sovereignty, Indigenous feminist scholar Leanne Betasamosake Simpson, in her book *As We Have Always Done*, observes that it

[1] Stéphane Couture and Sophie Toupin, "What does the notion of 'sovereignty' mean when referring to the digital?," *New Media & Society* 21, no. 10 (2019): 2305–22, https://doi.org/10.1177/1461444819865984.

was one of the first Indigenous movements in Canada to make extensive use of the Internet—through social media, blogs, and other digital tools—for mobilization.[2] In retrospect, however, Simpson became more critical, noting that the movement had not so much mobilized online as built a social media presence, which she saw as a different dynamic. It was, in part, Māori scholars who helped shift the discussion toward the idea of Indigenous digital and data sovereignty, and also the creation of the OCAP principles in 1998 by the First Nations Information Governance Center,[3] an organization located in Canada/the northern part of Turtle Island.

The discourse on digital sovereignty by state actors began to gain traction in the wake of Edward Snowden's revelations of mass surveillance and the Cambridge Analytica scandal. These events prompted a major reckoning in Europe, particularly after it was revealed that the U.S. government had spied on numerous European officials, including German Chancellor Angela Merkel. Snowden's revelations also prompted many civil society groups to reconsider the digital infrastructures they relied on and to think more critically about state surveillance. Hacker collectives and tech activists, who had long been developing autonomous digital infrastructures, suddenly found their work attracting heightened interest.

To summarize, some of our main findings were simple: First, a wide range of actors invoke the term *digital sovereignty*, but with very different meanings: states, civil society, and Indigenous peoples all use the term, though not in the same way. Second, the appeals for digital sovereignty by states other than the USA and by civil society are often framed in opposition to the U.S. and Silicon Valley, emphasizing the need to gain independence from American technology. Third, the type of digital sovereignty used by other states is largely against the dominance of USA over the Internet, meaning becoming independent from American tech.

*

Christoph: The paper was published in *New Media & Society* in 2019. Six years have passed since then—quite a long time considering technological shifts. What are your views on recent technological developments that have taken place since the paper was published: At which level do recent developments in AI (artificial intelligence), large language models (LLMs), machine learning, and synthetic data influence questions of digital sovereignty? Put differently, in your 2019 paper you outline "five perspectives on digital sovereignty." Might there be more today?

---

[2] Leanne Betasamosake Simpson, *As we have always done: Indigenous freedom through radical resistance* (University of Minnesota Press, 2017).

[3] OCAP is an acronym for the principles of data and information ownership, control, access, and possession.

Sophie: When we wrote our paper, AI had not yet taken the world by storm. AI existed but we had not yet gone through an AI-turn, so to speak. Today, governments and businesses are increasingly talking about "AI sovereignty" or "sovereign AI," a concept we would now need to include if we were to update our analysis. In a North American context, where we are located, threats about Canada's integration with the United States have felt very real in the winter of 2025. This has led to a new discourse around sovereignty, the digital and AI, which was less prominent in Canada/the northern part of Turtle Island than in Europe and other parts of the world. Governments and companies now use the term "sovereign AI" largely because it is currently fashionable, yet it carries multiple meanings rather than a single, fixed definition. Let us illustrate some of these interpretations.

The term sovereign AI has been used and popularized by Nvidia CEO Jensen Huang. Nvidia defines it as the following: "Sovereign AI refers to a nation's capabilities to produce artificial intelligence using its own infrastructure, data, workforce and business networks."[4] This is close to the definition given by Antoine Bosselut, who says that "AI sovereignty as the development, deployment, and governance of AI systems by a nation-state or trusted national institutions, with minimal reliance on foreign actors."[5] One of the cases in Canada that follows this definition is with the Canadian telecommunication company called Telus Corp. Telus, together with the USA-based Nvidia Corp. has positioned itself as developing sovereign AI factories. In the spring of 2025, the company announced the transformation of two data centers into two sovereign AI factories in Rimouski (Quebec) and Kamloops (British Columbia). We are told the Rimouski site "will be powered 99% by renewable energy sourced from Hydro-Quebec"[6]—a massive infrastructural project that itself faced major Inuit resistance in the 70s[7]—and in partnership with "Indigenous Peoples to help deliver positive social, cultural and economic outcomes through connectivity."[8] A lot of questions arise here. What does the implication of Nvidia as an American company do to Canadian Sovereign AI? How is the understanding of sovereign AI

[4] Angie Lee, "What is sovereign AI?," *Nvidia*, February 28, 2024, https://blogs.nvidia.com/blog/what-is-sovereign-ai.

[5] Antoine Bosselut, "Democratizing open LLMs for global sovereign AI applications," *YouTube*, May 2, 2025, https://www.youtube.com/watch?v=9qRSQCwh1Pk.

[6] "Telus, Nvidia announce plans to develop 'sovereign AI factory' in Quebec," Financial Post, March 18, 2025, last updated March 19 2025, https://financialpost.com/technology/telus-nvidia-develop-sovereign-ai-factory-quebec.

[7] Cf. Zebedee Nungak, *Wrestling with colonialism on steroids: Quebec Inuit fight for their homeland* (Véhicule Press, 2017).

[8] "AI that works for everyone: TELUS proud to join the UN AI for Good Global Summit 2025," Telus, News and Events, July 17, 2025, https://www.telus.com/en/about/news-and-events/media-releases/ai-that-works-for-everyone-telus-proud-to-join-un-ai-for-good-summit-2025.

factories by Telus different from that used by Mi'kma'ki and Wabanaki in Rimouski and Secwepemcul'ecw in Kamloops, on whose territories these factories are located? What will the impact be on the environment, especially the water consumption? Is Sovereign AI relying on digital/data workers/AI tutors from Canada to annotate the data that will train the AI models or from other countries in the world (Brazil, El Salvador, Morocco, etc.)? What are the conditions (financial and others) of these data workers? If they are trained by digital workers from outside Canada, can it still be called Sovereign AI?

One explanation as to why Sovereign AI or AI sovereignty is getting popular among countries such as Canada, European countries and elsewhere too is that AI has moved well beyond a toy technology. Foundational AI models are now running in defense and the military, banking and financial industries, in health care, among many other sectors. Governments are realizing that they need to control these technologies and the data that (as citizens) are driving our lives. If they don't build sovereign AI, then does it become a critical point of failure for them?

To a lesser extent, and in a somewhat dystopian view drawn from science fiction, Sovereign AI may mean that the technology will become "sovereign," that is, out of the control of humans.

I would like to end by mentioning "sovereign cloud," a term businesses (IBM, Oracle, etc.) have been using lately to mean that they can help an organization meet its digital sovereignty requirements. The simple fact that technology companies are creating a new service to help organizations reach digital sovereignty is a testament to the concept's wide use.

*

Christoph: Different interest groups interpret the concept of digital sovereignty differently. The term and the technologies associated with it have interpretative flexibility, so to speak, in a social constructivist sense. What does this mean for the technologies, platform policies, and data law aspects involved?

Stéphane: I believe people not only interpret what digital sovereignty means—they also perform it and construct it. What they say about sovereignty and technology can sometimes be incompatible. For example, when the European Union talks about sovereignty, it generally means that data should be hosted within their own countries and that governments should have control over the infrastructures hosting these data. In the case of authoritarian states like China and Russia, it can also mean that they should have technological and legal means to surveil their own citizens and control the information reaching them. In contrast, when civil society speaks of sovereignty, it often means resisting state surveillance and asserting control over personal data,

including protecting such data from private companies. What's important here is that these different sovereignties, or notions of sovereignty, can contradict one another. Similarly, different technologies can also be in conflict. One of the key challenges is: How do we navigate these conflicting sovereignties while also trying to build a shared world? How can we maintain a unified, less fragmented Internet? That's why some researchers are skeptical of the idea of digital sovereignty of certain states or regions (like the European Union)—because it can imply that every social group or entity seeks to control its own domain. Yet, it's also crucial to have common standards and universal principles. This debate around sovereignty echoes older questions about cultural diversity and, to some extent, relativism. How do we live in a common world while each group asserts its own sovereignty, its own way of knowing, its own reasons for acting? Because sometimes, what is presented as a universal principle may actually be a dominant one (not asserting our own sovereignty is de facto reinforcing the sovereignty of others upon ourselves).

Digital sovereignty, in this sense, can be understood as a sensitizing concept or a boundary object, if we use some notions in social science from Glenn Bowen[9] or Susan Leigh Star and James Griesemer.[10] It may not have a fixed or universally agreed-upon definition, but it evokes a shared sentiment—a general understanding of what it represents. This shared sentiment in relation to sovereignty is one thing we are trying to explore, while also refining the concept through theoretical work. Digital sovereignty draws on foundational principles such as autonomy, political self-determination, and these principles are broadly applicable and resonate across contexts, but they also require critical deconstruction. They transcend specific technologies, yet digital sovereignty is expressed and articulated differently depending on the infrastructures and systems in which it is embedded.

*

Christoph: In our everyday media and platform usage, it is difficult for us to understand the paths taken by the data we produce, which data centers these data are sent to, and how these data are algorithmically processed (with all the included biases) in order to analyze, evaluate, classify, and economize our actions and predict future behavior. Can we even know whether we are digitally sovereign on an individual level?

[9] Glenn A. Bowen, "Grounded theory and sensitizing concepts," *International Journal of Qualitative Methods* 5, no. 3 (2006): 12–23, https://doi.org/10.1177/160940690600500304.

[10] Susan Leigh Star and James R. Griesemer, "Institutional ecology, 'translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39," *Social Studies of Science* 19, no. 3 (1989): 387–420.

Sophie: With commercial extractive generative AI (also called commercial LLMs), it is more and more difficult to have our individual and collective data sovereignty respected. It is not only a matter of knowing the paths that the data we produce follow, which is in and of itself difficult by design, but it is also the fact that AI scrapers have captured our data. AI scrapers are automated bots that trawl the websites of governments, universities, media outlets, researchers and even private individual content to feed the databases needed to develop generative AI models. OpenAI, the developer of ChatGPT, was one of the first companies to use AI crawlers or scrapers to amass as much data as possible to train its GPT model. Only on August 7, 2023 did OpenAI publish a method for blocking its own bot, GPTBot, thereby preventing data collection via what is known as a robots.txt file. Such a file allows website creators, government institutions and media outlets to define the rules for accessing their online content. However, this initiative came after GPTBot had already crawled most of the web to build the training data for its models.[11] For many observers, this amounts to a form of massive data capture, carried out without explicit consent and often without the knowledge of the authors and administrators of the sites. The generative AI products available to us today are therefore largely based on the collection of collective knowledge from the web, built up over decades by millions of contributors. This brings to the fore important questions: To what extent and in which context should companies (tech, but also others) be able to innovate with "our data" and/or data that were taken from the Internet and might be copyrighted (media outlets, books from shadow libraries, etc.)? What do we do with these datasets and the tools they helped create?

Stéphane: It's important to remember that, even in digital environments, consent remains a relative concept. This has been widely discussed both in public discourse and in academic research. In practice, very few people read the terms of consent carefully—especially when it comes to proving something or accessing a service. Because these documents are often long and complex, users tend to approve everything without fully understanding what they're agreeing to.

Moreover, there are consequences to not consenting. Refusing consent can mean being excluded from dominant social media platforms, and thus from participating in broader digital culture. This raises important questions about the actual possibility of meaningful consent in social networks. Some alternative platforms and protocols are trying to address this issue by proposing more nuanced models of consent—not just whether one participates in a network, but whether one consents to share or receive specific types of content. This is, for instance, one of the ideas

[11] Cf. David Pierce, "The text file that runs the internet," *The Verge*, February 14, 2024, https://www.theverge.com/24067997/robots-txt-ai-text-file-web-crawlers-spiders.

proposed by Christine Lemmer-Webber, the creator of the ActivityPub protocol, which underpins Mastodon and many of the platforms of Fediverse. She advocates for what she calls "networks of consent,"[12] which allow communities to reclaim control over their digital environments. We explore this in a paper we are about to publish in French.

We've also seen examples of collective digital sovereignty in action. For instance, in the case of Google Sidewalk Labs, the community ultimately rejected the project, exercising a form of collective refusal and asserting their sovereignty over urban data and infrastructure.

Now, when it comes to bodily sovereignty, the stakes are often more individual. But what interests me most in the context of digital sovereignty is its collective dimension. In many cases, individual sovereignty is not sufficient—we need to think about how communities can assert control together.

*

Christoph: Sophie, you remind us[13] that Gabriella Coleman defines a hack as "a clever technical solution arrived at through non-obvious means,"[14] also for (re)appropriating technologies or infrastructures and eventually turning them into infrastructures of autonomy, to exist outside a dominant oppressive system, that is. And, more specifically, you refer to a technological encryption system for secure and secret communication (the autonomous encrypted communication network, AENC), a communication system rooted in hacker practice. Could you tell us how the system worked and what implications such a system has for issues of digital sovereignty?

Sophie: During my PhD research, I examined an encrypted communication network developed in the 1980s and 1990s by the Technical Committee of the South African Communist Party (SACP) and the African National Congress (ANC). This committee successfully built an autonomous, encrypted communication network that enabled secure and transnational coordination in the face of apartheid-era oppression, violence, and surveillance. South African techies and their allies from the African continent, Canada, the Netherlands and Britain, among others, dedicated years to mastering digital encryption and establishing transnational messaging capabilities. At

[12] Christine Lemmer-Webber, "OcapPub: Towards networks of consent," *GitLab*, December 12, 2024, https://gitlab.com/spritely/ocappub/blob/master/README.org.

[13] Sophie Toupin, "Gesturing towards anti-colonial hacking and its infrastructure," *Journal of Peer Production* 9 (2016), http://peerproduction.net/editsuite/issues/issue-9-alternative-internets/peer-reviewed-papers/anti-colonial-hacking, accessed October 29, 2025.

[14] Gabriella Coleman, "Hackers, liberalism, and pleasure," *Institute for Advanced Study, Social Science*, 2011, accessed October 29, 2025, https://www.ias.edu/ideas/coleman-hackers.

the time, computers were far from widespread, and most people did not know how to use them. To overcome these challenges, they trained a handful of activists, wrote how-tos and strategically infiltrated laptop computers across multiple South African cities, among other countries (Zambia, etc.).

When freedom fighters wanted to send a message through this newly built system, they typed it on the infiltrated computer and used an encrypted floppy disk (also infiltrated) to encrypt the message. It was then passed through the computer's serial port to an acoustic coupler modem. The digital data was thus converted into sound, and it was captured on a small cassette tape recorder. The tape player was then played on to an outside landline phone and sent to London, where another freedom fighter was located. The person in London decrypted the message and decided where to send it: either to Lusaka, Zambia, where the leaders of the ANC were, to Amsterdam or to Tall Cree, an indigenous reserve in Canada where activists were located to support the struggle.

While some of its operators refer to the encrypted communication network as the "ANC Internet," the system was not fully sovereign or autonomous in the strict sense. It was built on existing public and private digital infrastructures from Europe and North America—such as the international telephone network and telematics—which shaped its technical possibilities and limitations. What made this system innovative was not the creation of entirely new infrastructure (this would have been impossible and too lengthy as an endeavor), but rather the way heterogeneous technologies spoke to each other to enable secure, transnational communication under apartheid-era surveillance and repression. Although the concept of "digital sovereignty" was not in use at the time, today this framework helps us understand the significance of what the Technical Committee built. The expression gestures to what can now be understood as a civil society-led digital sovereignty—an infrastructure constructed and controlled by activists, even if it relied on existing networks and infrastructures. In this sense, what the Technical Committee did aligns with what we consider today as an expansive understanding of digital sovereignty: not as complete independence from global systems and infrastructures, but as the ability to repurpose and govern digital tools in the service of political autonomy and resistance.

*

Christoph: Stéphane, your research focuses on free software, decentralized networks and other community-based platforms, among others, with a strong focus on aspects of design. Is digital sovereignty also a question of design? If so, by whom, and for what reasons can digital sovereignty be designed? At what different levels (or scales) is digital sovereignty also a question of design?

Stéphane: Yes, I believe this is fundamentally a question of design—not only in terms of interface or user experience, but also in terms of infrastructure: where data is stored, who builds the technology, and how choices are presented to users. Take a simple example: When using a cloud service like Amazon Web Services, users are asked to choose the location of their server. This is a design decision. And it's not just about whether users are asked, but *how* they are asked. The same applies to consent. For over fifteen years, I (and many others) have been concerned with the complexity and opacity of consent forms, license agreements, and similar documents. People routinely sign them without understanding their implications. So how can sovereignty be asserted in such contexts—when systems are too complex, and the burden of comprehension is too high?

This is why we need to design technologies in ways that allow individuals and communities to perform and constitute their sovereignty. If only centralized technological options are available, it becomes extremely difficult for individuals to resist or respond to that centralization. The issue is not only technical—it is also cultural. In Quebec, and more broadly in Canada, cultural sovereignty is a major concern. It refers to the desire to protect local culture and ensure that a meaningful proportion of cultural content is visible on television and digital platforms. But if the design of those platforms does not support the discovery of such content, then sovereignty is undermined. Sovereignty, in this sense, is not only a matter of policy—it is embedded in design choices.

*

Christoph: You two have, among others, a current research project that runs until 2029, entitled "Résistances numériques: Théorisation du concept et cartographie des pratiques" and the project "(Re-)claiming digital sovereignty in discourse, policy and practice," running until 2028, in which shifting power relations and geopolitical tensions are key issues of investigation. Could you tell us a bit more about these projects and how you approach issues of digital sovereignty? The second project seems to focus more on nation-state dimensions, while the first focuses more on self-organized or collective practices. Why is it important to consider both?

Sophie: Stephane is the principal investigator (PI) on both projects and Sophie is a co-researcher along with a few other scholars. Both projects are funded in whole or in part by the Social Sciences and Humanities Research Council (SSHRC), the Canadian research funding agency that promotes and supports research and research training in the humanities and social sciences.

During the pandemic, we started getting interested in the term digital resistance. Stephane was asked by a journal called *Revue Possibles* to edit a special issue on

digital resistance, a term that neither of us were using at the time. He invited me to be a co-editor. For the introduction to this special issue, we conducted an initial exploration of certain digital resistance practices, such as the creation of alternative infrastructures (to challenge large corporations, promote autonomy, or oppose authoritarian regimes) or, on a more tactical level, cooperation among platform users to outsmart algorithms. We came to understand that in English, the concept of "digital resistance" was conceptualized at the turn of the millennium by the Critical Art Ensemble (CAE) collective (2001). The group based it on the idea of "tactical media," a concept that refers to critical uses and theorizing aimed at promoting various subversive practices.[15] One of the models put forward at the time was that of "electronic civil disobedience," which aimed to mobilize digital technologies for protest purposes in order to disrupt the powers that be.[16] It should be noted that the CAE had developed a small, easy-to-use denial-of-service (DDoS) attack software to paralyze the websites of the Mexican government, which at the time was repressing the Zapatista movement in Chiapas.

Now, the concept of digital resistance is regularly used in academic and activist writings to describe practices involving the use, repurposing and/or creation of content and/or technologies, most often—but not always—from a progressive and anti-oppressive perspective. It is associated with practices that are often tactical rather than strategic and, by definition, opposed to a certain dominant and hegemonic order. This is why today we see the term digital resistance being claimed by reactionary movements. However, the history of this term is firmly rooted in an anti-oppressive approach.

More recently, because of the political context, many actors have been using the term digital resistance, not only tech collectives and activists, but also Indigenous people, feminist groups, small companies, and even states who want to defy the hegemony of Silicon Valley aligned with the USA administration, and what some call technofascism.

The second research project called "ClaimSov: (Re-)claiming digital sovereignty in discourse, policy and practice" is funded by the Open Research Area, a collaborative international research funding initiative aimed at supporting joint research projects in the social sciences and humanities across multiple countries—in our case, Germany, France, and Canada. We are working with Julia Pohle (main PI in Germany) and Francesca Musiani (PI in France). The goal of the project is to provide

[15] Critical Art Ensemble, "Tactical media," accessed October 29, 2025, http://critical-art.net/category/tactical-media.

[16] Cf. Critical Art Ensemble, "Electronic civil disobedience," accessed October 29, 2025, http://www.critical-art.net/books/ecd.

systematic theoretical and empirical research on digital sovereignty-related discourses and governance mechanisms in national and supranational contexts in three key geopolitical blocks: 1) the European Union, both at the EU level and within France and Germany, 2) North America (with a focus on the United States and Canada), and 3) Russia and China.

One of the ways to connect digital resistance to digital sovereignty is to understand the latter through the lens of the former. In other words, digital sovereignty can be conceived as a form of digital resistance and all actors can and are using these tactics.

Stéphane: Apart from deepening the analysis of digital sovereignty discourses across different regions, one of the things we are trying to grasp in the ClaimSov project is the difference between digital sovereignty discourses and how they are enacted in practice—for instance, through policy or infrastructure. But we are only just starting this project, and we aim to take an inductive approach, so we might come up with other interesting and original perspectives.

Concerning resistance and sovereignty, I think there is a conceptual transition from the former to the latter. Resistance is often a reactive practice—it implies a defensive posture, a subaltern position. We resist something imposed upon us. Sovereignty, on the other hand, is also relational—we are sovereign in relation to others, whether individuals, institutions, or states—but it represents a more affirmative stance. As we've seen, the countries that assert sovereignty in the digital realm are usually not the dominant power (i.e., the United States), but what I would call secondary powers, such as Europe or the BRICS countries. They assert sovereignty precisely because they are not dominant. Sovereignty, then, is not merely resistance—it is a positive affirmation, a way of going beyond reaction to propose and enact alternatives. This shift from resistance to sovereignty is, I believe, an important conceptual transition that deserves attention.

I'm interested in exploring different concepts such as digital resistance, digital sovereignty, and also solidarity. What do these concepts actually mean, and what kinds of problems do they address? On a more empirical and political level, many people recognize that digital technologies have become a central issue. In response, they try—at least in the realm of imagination—to find ways to avoid harm or to escape certain technological constraints. Digital resistance, in this sense, is a "sensitive" concept: it may lack precise definition, but it sensitizes us to certain practices and experiences. Sovereignty might also be understood as a sensitive concept—less clearly defined, but nonetheless generative. It helps us trace certain dynamics and formulate

responses. It's not only about critique—it's about action and propositions. It's not just about resisting dystopia or surveillance—it's about building non-dystopian worlds.

This transition is important to me personally. It's not just about critique—it's about action and propositions. In both resistance and sovereignty, we move beyond critique to examine how people act—what they do to maintain or reclaim power. These concepts invite us to look at practices of agency, of self-determination, and of collective imagination.

*

Christoph: Recently, several works have been published on Indigenous data sovereignty. You also addressed this topic in 2019. What makes this topic so special and so important, even though it is often underrepresented in the discourse in quantitative terms?

Stéphane: Well, I'm not sure Indigenous digital sovereignty is that underrepresented—it obviously depends on where you look. In Canada, for instance, it's not the dominant discourse, but it is certainly a significant one, including in quantitative terms. I imagine the same could be said for Australia. But as you noted, it's also important in qualitative terms, for two main reasons.

First, it is politically significant. In settler colonial countries such as Canada, the United States, or Australia, we are in a period where many people are aiming toward reconciliation. Universities and governments have launched numerous initiatives to acknowledge past injustices and to recognize the right to self-determination of Indigenous peoples. In this context, interest in Indigenous digital sovereignties is politically anchored. It is important to understand these perspectives, especially since governments—like the Government of Canada—have begun to refer to Indigenous data sovereignty in their discourses. However, they often do so while maintaining that Indigenous sovereignty does not entail returning land. This reveals a tension: Is sovereignty merely discursive, or does it carry practical implications?

Second, there is a conceptual dimension. Indigenous scholars and activists have developed rich and multidimensional understandings of Indigenous digital and data sovereignty. These go far beyond the narrow notion of data storage, which tends to dominate European and non-Indigenous Canadian policy frameworks. Their conceptualizations include critiques of extractive and colonial research methodologies—methods that fail to respect Indigenous cultures, languages, and epistemologies. For example, some researchers have historically sought to commodify traditional knowledge, such as medicinal remedies. Others have collected data on health or social issues within Indigenous communities without ensuring that these communities retain control over the data or their use—for instance, to ensure that results coming

out of these data are used to improve their community and not to stigmatize or control them. Indigenous sovereignty, in this sense, extends to the production of data itself—a dimension often overlooked in dominant frameworks.[17]

It is important to emphasize that we are not Indigenous ourselves. Many Indigenous scholars are already publishing on these topics. Our goal is not to speak on their behalf, but to help make these contributions better known. It's a delicate position: We want to valorize Indigenous knowledge without appropriating it or replacing Indigenous voices. That's why it's essential to integrate not only Indigenous perspectives, but also to create space for Indigenous thinkers to participate directly in these conversations.

*

Christoph: Questions of digital sovereignty have an inherent geopolitical dimension, for example, because data centers and server farms are tied to physical locations and environments and require material infrastructure, such as fiber optic networks in which signals are transmitted—despite all the fluid cloud metaphors. The *Undersea Network*[18] also has something to do with issues of digital sovereignty, but questions in this regard also affect the Global South in a particular way. Can you tell us something about the relationship between the Global South and aspects of digital sovereignty?

Stéphane: I would like to refer here to Min Jiang and Luca Belli's book on digital sovereignty in BRICS countries, which offers a comprehensive and well-structured overview of the topic.[19] My reflection fits within broader discussions on what is commonly referred to as the Global South. However, it is important to critically examine what this term actually encompasses. Some scholars argue that Indigenous peoples in the North should be considered part of the Global South from a political-economic perspective. This raises important questions about the boundaries and assumptions embedded in geopolitical categories.

While many of the challenges faced by BRICS countries may resemble those encountered in European contexts—particularly in terms of digital governance and infrastructure—they are also shaped by distinct colonial and postcolonial dynamics. These include the cultural domination of the North over the South, a phenomenon already highlighted in the MacBride Report and by critical scholars such as Herbert Schiller. These authors have pointed to the structural asymmetries in global media

[17] Cf. e.g. Tahu Kukutai and John Taylor, eds., *Indigenous data sovereignty. Toward an agenda* (ANU Press, 2016).

[18] Cf. Nicole Starosielski, *The undersea network* (Durham and London, 2015).

[19] Min Jiang and Luca Belli, eds., *Digital sovereignty in the BRICS countries. How the Global South and emerging power alliances are reshaping digital governance* (Cambridge University Press, 2025).

flows and the symbolic power exercised through cultural production and representation. In this sense, digital sovereignty in the Global South cannot be understood solely through the lens of technological autonomy. In a similar way to Indigenous Digital Sovereignty, it must also be situated within broader struggles over epistemic justice, cultural self-determination, and the decolonization of digital infrastructures.

*

Christoph: In media studies, we have been noticing a shift from media to data research for some time now. Since it makes less and less sense to talk about individual, clearly separate media, but rather about media environments networked via data, does it make sense to speak of digital sovereignty any longer? Or, conversely, is the concept becoming increasingly important as a result? In our post-digital ecology, the digital is everywhere anyway (at least within the Global North): What would distinguish the concept of data sovereignty from digital sovereignty? Would "algorithmic sovereignty" be a meaningful extension of the concept?

Stéphane: I'm not really approaching this from a perspective of concept purification, to use Latour's term.[20] For instance, would the term algorithmic sovereignty or technological sovereignty be preferable to digital sovereignty? That's not my primary concern. What interests me are the manifestations of sovereignty discourse within a digital context. Of course, if one wants to specify the type of sovereignty or its object—whether it's algorithms, data, or something else—that's certainly possible, but it's not my starting point.

What I really appreciate about the concept of sovereignty is its fundamentally political and collective nature. Of course, there are certain currents, like that of the "sovereign citizen," which emphasize the individual. But generally speaking, sovereignty is understood at the level of a collective or a group, not an individual. This sovereignty can be expressed in different ways. For example, when a general assembly makes a decision, it acts as a sovereign instance within a given collective.

In the context of the Internet, the question becomes: Which "collective" is this sovereignty associated with? Often, we think of the state. But what we observe in civil society practices—among certain hackers or activists—is the formation of collectives that seek to establish their own modes of governance over specific digital objects. What we see, then, are sociotechnical arrangements grounded in community-based, often exclusive foundations, through which a form of autonomous governance is exercised.

[20] For a schematization of the concept see e.g. diagram "purification and mediation" in Bruno Latour, *We have never been modern*, trans. Catherine Porter (Harvard University Press, 1993), 51.

*

Christoph: You remind us that the concept of sovereignty is rooted in the Western history of colonialism and imperialism. You follow this up with a question. I want to quote your concluding sentence from the 2019 paper and turn it into a question for you: "So the question is then: what is to be gained and to be lost in the use of sovereignty when thinking about the digital?"[21]

Stéphane: This also brings us back to Indigenous perspectives, where the very notion of sovereignty is often contested. Scholars such as Taiaiake Alfred,[22] for instance, argue that the concept of sovereignty is inherently colonial. To speak of sovereignty, he suggests, is to implicitly adopt a colonial framework of thought. From this standpoint, invoking sovereignty may reinforce the very structures of domination that Indigenous communities seek to dismantle.

Moreover, Alfred notes that Indigenous groups are unlikely to become "states" in the conventional sense—that is, sovereign entities recognized within the Westphalian order. This raises the question: Why retain the term sovereignty at all? Would it not be more productive to explore alternative conceptual vocabularies to articulate struggles for autonomy?

Yet, other Indigenous thinkers argue in favor of retaining the term. For them, sovereignty remains a powerful and mobilizing concept—one that gestures toward self-determination and greater autonomy. It is not merely a theoretical construct but a political horizon that continues to inspire collective action. This tension reveals what is gained and what is potentially lost in the use of the term.

A similar dynamic can be observed in civil society collectives engaged in digital activism. As we noted in our 2019 article, many of these groups engage in practices akin to those found in the free software movement—developing autonomous infrastructures and open-source tools. However, rather than framing these efforts in terms of software freedom, they increasingly speak of digital sovereignty or sovereign infrastructures.

What is gained in this shift is a more overtly political discourse, one that is rooted in self-determination and resonates with broader struggles for autonomy. It

[21] Couture and Toupin, "Notion of 'sovereignty,'" 2319.

[22] Cf. e.g. Gerald R. [Taiaiake] Alfred, *Heeding the voices of our ancestors. Kahnawake Mohawk politics and the rise of native nationalism* (Oxford University Press, 1995); Taiaiake Alfred, *Wasáse: Indigenous pathways of action and freedom* (University of Toronto Press, 2005); Taiaiake Alfred, *It's all about the land. Collected talks and interviews on indigenous resurgence*, ed. Ann Rogers (University of Toronto Press, 2023).

speaks to audiences who may not be familiar with the technical or ideological foundations of free software, but who recognize the stakes involved in reclaiming control over digital environments. In this sense, sovereignty functions as a term that travels across domains, carrying different meanings but enabling shared conversations.

*

Christoph: As a somewhat speculative final question: Issues of digital sovereignty have always had a clear connection to human subjects in the end, this also applies to the discourse at the state level. The discussion on digital sovereignty is therefore anthropocentric at its core, even when it comes to issues of technological infrastructure, data law, data protection, etc. In a different twist of the term, and if we take the concepts of actor-network theory seriously and also include current more-than-human approaches, do non-human actors (e.g. AI actors) also have a right to being sovereign?

Sophie: Personally, I would not give the same kind of symmetrical sovereignty to AI as to non-humans entities such as the Earth, flora, fauna, and human beings. One of the main reasons is that AI, algorithms and datasets are produced by humans. These are not entities that have developed by themselves. Depending on your theory of history, the Earth and its ecosystems possess (elements) sovereignty, though because of our negligence, exploitation and non-caring, non-humans have been altered by us. In my current thinking, I am inclined to challenge and deprivilege the discourse on the sovereignty of AI. This narrative too often echoes Silicon Valley's portrayal of AI as sentient—a framing that risks misleading the public about what AI actually is. Rather than clarifying, it obscures the fundamentally human-driven nature of these technologies and their embedded power dynamics. Karen Hao's new book *Empire of AI: Dreams and Nightmares in Sam Altman's OpenAI*[23] explains this very well.

Stéphane: I tend to agree with Sophie here: It is crucial to approach these questions from a situated, rather than an abstract or universal perspective. Lucy Suchman, in *Human-Machine Configurations*, has already raised a similar concern, noting that "the technical"—and particularly AI systems—are often privileged and granted significant agency through funding and political support for their developers, while "the social" is frequently relegated to the margins.[24] While the idea of symmetrical sovereignty between humans and non-humans may be theoretically appealing, it risks reinforcing the power of entities that are already dominant. This raises important questions about the political implications of such a move.

---

[23] Karen Hao, *Empire of AI: Dreams and Nightmares in Sam Altman's OpenAI* (Penguin Press, 2025).

[24] Cf. Lucy Suchman, *Human-machine reconfigurations. Plans and situated actions*, 2nd edition (Cambridge University Press, 2007), 269–70.

That said, I remain deeply influenced by Bruno Latour's work, especially his efforts to explore how nature—as a non-human actor—might be granted agency, and even, in the context of this discussion, sovereignty.[25] This idea is compelling as it invites us to think beyond anthropocentric frameworks and consider what it might mean for nature to attain a form of stability that could be interpreted as sovereign.

Latour's work also prompts us to ask: Who has the authority to speak in the name of nature's sovereignty? Who holds the legitimacy to represent its interests? These are politically charged questions, especially given that nature does not speak in human language—it communicates through catastrophes, through scientific data, through ecological transformations. Imagining the Earth as sovereign—a sovereign Earth—opens up a provocative space for reflection.

This concept carries both promise and risk. On the one hand, it could help reframe ecological politics in terms of rights, agency, and representation. On the other, it risks being appropriated by actors who claim to speak for nature without accountability. Still, I believe there is value in this gesture—in thinking of sovereignty not only as a human or state-based construct, but as something that might extend to the non-human world.

[25] Cf. e.g. Bruno Latour, *Politics of nature: How to bring the sciences into democracy*, trans. Catherine Porter (Harvard University Press, 2004).

Bibliography

Alfred, Gerald R. [Taiaiake]. *Heeding the voices of our ancestors. Kahnawake Mohawk politics and the rise of native nationalism*. Oxford University Press, 1995.

Alfred, Taiaiake. *Wasáse: Indigenous pathways of action and freedom*. University of Toronto Press, 2005.

Alfred, Taiaiake. *It's all about the land. Collected talks and interviews on indigenous resurgence*. Edited by Ann Rogers. University of Toronto Press, 2023.

Bosselut, Antoine. "Democratizing open LLMs for global sovereign AI applications." *YouTube*, May 2, 2025. https://www.youtube.com/watch?v=9qRSQCwh1Pk.

Bowen, Glenn A. "Grounded theory and sensitizing concepts." *International Journal of Qualitative Methods* 5, no. 3 (2006): 12–23. https://doi.org/10.1177/160940690600500304.

Coleman, Gabriella. "Hackers, liberalism, and pleasure." *Institute for Advanced Study, Social Science*, 2011, accessed October 29, 2025. https://www.ias.edu/ideas/coleman-hackers.

Couture, Stéphane, and Sophie Toupin. "What does the notion of 'sovereignty' mean when referring to the digital?" *New Media & Society* 21, no. 10 (2019): 2305–22. https://doi.org/10.1177/1461444819865984.

Critical Art Ensemble. "Electronic civil disobedience." Accessed October 29, 2025. http://www.critical-art.net/books/ecd.

Critical Art Ensemble. "Tactical media." Accessed October 29, 2025. http://critical-art.net/category/tactical-media.

Financial Post. "Telus, Nvidia announce plans to develop 'sovereign AI factory' in Quebec." March 18, 2025, last updated March 19 2025. https://financialpost.com/technology/telus-nvidia-develop-sovereign-ai-factory-quebec.

Hao, Karen. *Empire of AI: Dreams and Nightmares in Sam Altman's OpenAI*. Penguin Press, 2025.

Jiang, Min, and Luca Belli, eds. *Digital sovereignty in the BRICS countries. How the Global South and emerging power alliances are reshaping digital governance*. Cambridge University Press, 2025.

Kukutai, Tahu, and John Taylor, eds. *Indigenous data sovereignty. Toward an agenda*. ANU Press, 2016.

Latour, Bruno. *We have never been modern*. Translated by Catherine Porter. Harvard University Press, 1993.

Latour, Bruno. *Politics of nature: How to bring the sciences into democracy*. Translated by Catherine Porter. Harvard University Press, 2004.

Lee, Angie. "What is sovereign AI?" *Nvidia*, February 28, 2024. https://blogs.nvidia.com/blog/what-is-sovereign-ai. Accessed October 29, 2025.

Lemmer-Webber, Christine. "OcapPub: Towards networks of consent." *GitLab*, December 12, 2024. https://gitlab.com/spritely/ocappub/blob/master/README.org.

Nungak, Zebedee. *Wrestling with colonialism on steroids: Quebec Inuit fight for their homeland*. Véhicule Press, 2017.

Pierce, David. "The text file that runs the internet." *The Verge*, February 14, 2024. https://www.theverge.com/24067997/robots-txt-ai-text-file-web-crawlers-spiders. Accessed October 29, 2025.

Simpson, Leanne Betasamosake. *As we have always done: Indigenous freedom through radical resistance*. University of Minnesota Press, 2017.

Star, Susan Leigh, and James R. Griesemer. "Institutional ecology, 'translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39." *Social Studies of Science* 19, no. 3 (1989): 387–420.

Starosielski, Nicole. *The undersea network*. Durham and London, 2015.

Suchman, Lucy. *Human-machine reconfigurations. Plans and situated actions*. 2nd edition. Cambridge University Press, 2007.

Telus. "AI that works for everyone: TELUS proud to join the UN AI for Good Global Summit 2025." July 17, 2025. https://www.telus.com/en/about/news-and-events/media-releases/ai-that-works-for-everyone-telus-proud-to-join-un-ai-for-good-summit-2025. Accessed October 29, 2025.

Toupin, Sophie. "Gesturing towards anti-colonial hacking and its infrastructure." *Journal of Peer Production* 9 (2016). http://peerproduction.net/editsuite/issues/issue-9-alternative-internets/peer-reviewed-papers/anti-colonial-hacking. Accessed October 29, 2025.