



# What does the notion of “sovereignty” mean when referring to the digital?

new media & society

2019, Vol. 21(10) 2305–2322

© The Author(s) 2019

Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/1461444819865984

journals.sagepub.com/home/nms



**Stephane Couture** 

York University, Canada

**Sophie Toupin**

McGill University, Canada

## Abstract

This article analyzes how the notion of “sovereignty” has been and is still mobilized in the realm of the digital. This notion is increasingly used to describe various forms of independence, control, and autonomy over digital infrastructures, technologies, and data. Our analysis originates from our previous and current research with activist “tech collectives” where we observed a use of the notion to emphasize alternative technological practices in a way that significantly differs from a governmental policy perspective. In this article, we review several publications in order to show the difference, if not diverging ways in which the notion is being conceptualized, in particular by different groups. We show that while the notion is generally used to assert some form of collective control on digital content and/or infrastructures, the precise interpretations, subjects, meanings, and definitions of sovereignty can significantly differ.

## Keywords

Data sovereignty, digital sovereignty, discourses, indigenous peoples, Internet governance, nation-states, social movements, technological sovereignty

---

## Corresponding author:

Stephane Couture, Bilingual Program in Communications, Glendon College, York University, 2275 Bayview Avenue, Toronto, ON, Canada M4N 3M6.

Email: [stephane.couture24@gmail.com](mailto:stephane.couture24@gmail.com)

## Introduction

This article aims at examining the notion of sovereignty as it applies to “the digital.” By “digital” we refer to its conventional definition, meaning technologies, infrastructures, data, and content based on and/or using electronic computing techniques (Peters, 2016: 94). As shown in Table 1, there has been an increased use in recent years of the notion of “sovereignty” in relation to such terms as “digital,” “data,” and “technology.” More importantly for this article, the notion of “sovereignty” in relation to the digital is now mobilized by a diversity of actors, from heads of states to indigenous scholars, to grass-roots movements, and anarchist-oriented “tech collectives,” with very diverse conceptualizations, to promote goals as diverse as state protectionism, multistakeholder Internet governance or protection against state surveillance.

In this article, we examine different ways in which sovereignty has been conceptualized by different types of actors in relation to the digital. Our analysis is grounded in our respective ethnographic fieldwork and engagement, as co-authors, within tech activist and hacker collectives oriented toward social justice (Couture et al., 2016; Couture, 2018; Toupin, 2014). In the past few years, we have witnessed some of these groups use the concept of “technological sovereignty” to describe practices of developing digital technologies and infrastructures, using free software, servers, and encryption-based technologies, both at the collective and individual levels (Beltrán, 2016; Haché, 2014a, 2014b, 2017; Nitot, 2016). We were particularly intrigued by this use of the notion as it significantly differs from the more dominant policy-oriented and state-centric perspectives. The use of the term “sovereignty” was even more surprising to us as these activists had themselves been critical of the notion by associating it with “state sovereignty” rather than “autonomy.” With this in mind, we decided to dig deeper to find out who is using the notion, how it is being used and why. It is thus through our involvement with tech activists (oriented toward social justice) that we decided to look at its use within a broader range of actors and explore why these groups (and others) are articulating technology through “sovereignty.” While grounded in these participatory engagements, our project is closer to discourse analysis and aims at showing the diversity of use of the notion of sovereignty as it relates to the digital, especially in state-centric approaches and other levels of collective organizations (such as social movements and indigenous peoples).

This article, therefore, is not a systematic and exhaustive review of all material published on the subject but rather a critical survey of some writings chosen along the lines of our interest toward a critique of the notion of sovereignty. Moreover, our analysis is

**Table 1.** Frequency of use of the notion of “sovereignty” as related to the digital (using ProQuest Central).

	Data sovereignty		Technological sovereignty		Digital sovereignty	
	Academic	Other	Academic	Other	Academic	Other
Before 2011	0	23	12	81	0	6
2011–2014	18	794	6	101	2	49
2015–2018	89	2459	20	131	22	239

limited to articles in English, with some French references. To choose these publications, we did an initial broad survey of academic articles, books, and other publications using academic databases such as Google Scholar, WorldCat, and our respective university library catalogs. Furthermore, we used Google search to get a sense of what was out there in terms of online newspapers and activist publications, among others. While we started our search with the term “technological sovereignty”—as witnessed with tech activists—we also used other keywords related to the digital, such as “digital sovereignty,” “network sovereignty,” “data sovereignty,” “spectrum sovereignty,” “computer sovereignty,” and “information sovereignty.” Through this methodological process, we collected a first set of about 50 documents, including academic articles and books. After surveying and reading these documents, we created a rough set of clusters along some conceptual categories representing several types of actors: established states, indigenous nations, civil society and social movements, and what we call individual personhood. Following this first categorization, we summarized our collected material and added new documents using a snowball sampling approach. We later added another category to reflect the early perspective—which is still present today—that communication networks and the Internet more specifically extend beyond state sovereignty and that, for this reason, should be governed by their own people.

We recognize that our approach is far from extensive. While a more systematic and quantitative analysis of the literature would certainly be interesting, this is not the approach we took.<sup>1</sup> It is rather a qualitative analysis of a specific but limited set of (academic and nonacademic) articles and books on the subject that exemplify the various interpretations, meanings, and ideological values attached to the notion of sovereignty as related to the digital. A primary methodological rule we observed was to choose texts and analyses that explicitly used (in their title, abstract, or body) the term sovereignty in the context of the digital. We avoided interpreting statements that we could have implicitly understood to refer to digital sovereignty.

From an analytical perspective, our article is influenced by Proulx’s (2007) study on the discourses surrounding the term “information society” between the 1970s and the early 2000s. Proulx (2007) develops from Krippendorff’s (1993) constructivist approach on the use of metaphors and writes that “any metaphor, any term employed by social actors to describe an existing or perceived reality can be susceptible to being an object of controversy” and that “metaphors organize categories with which subjects think” (Proulx, 2007: 113, our translation). Using this approach, the author looks at what he calls the “metaphor of an information society” to map the different actors using this term and their occasional diverging ideological goals (Proulx, 2007: 113, our translation). Following this perspective, our aim is to interrogate the “politics of the concept” and to examine how these publications talk about sovereignty, who the people involved in these discourses are, and what their political-ideological objectives are. This article aims to answer the following questions: how is the notion of “sovereignty” mobilized to understand digital data, content, and/or infrastructures? How does this notion relate (or not) to more traditional notions of nation-state sovereignty or to other interpretations of sovereignty implicit in the normative concepts of social justice, autonomy, or collective governance?

In this article, we first problematize the notion of sovereignty by briefly reviewing its different historical and epistemological conceptualizations. Second, we examine different perspectives in which the notion of sovereignty has been used by various actors, such as established states, indigenous nations, social movements, in addition to more abstract actors like “the individual” and the “people of the Internet.” Third, we briefly discuss the distinctions and commonalities between these diverse interpretations and show that while the notion is generally used to assert some form of collective control on digital content and/or infrastructures—and often in resistance to some form of hegemony—the precise interpretations, subjects, meanings, and definitions of sovereignty can significantly differ from one group to another.

## Problematizing sovereignty

Before analyzing the use of “digital sovereignty” and related notions, we first look at how the notion of “sovereignty” (without reference to the digital) has been historically and epistemologically conceptualized. The contemporary notion of sovereignty as it relates to the digital reflects and refers to these varying conceptualizations, ranging from the collective to the individual. This plurality is also reflected by the diverse set of actors who use this notion according to varying perspectives.

While the term sovereignty has been used since the era of ancient Romans (Hinsley, 1986), its modern use as it relates to the state is often associated with such authors as Machiavelli, Hobbes, Bodin, and later, Schmitt. Sovereignty is generally defined as the supreme authority over a political entity (a polity). In the *Stanford Encyclopedia of Philosophy*, Philpott (2003: 3) defines four principles for the sovereign: (1) it possesses authority; (2) this authority is derived “from some mutually acknowledged source of legitimacy”—which can be God, a constitution, or a hereditary law; (3) this authority is supreme; and (4) this authority is over a territory. Concerning territory, Hollis (2012) remarks that the label “territory” should not only be restricted to landmass but also to resources in the bounded space such as human infrastructures, air space, or minerals (or oil) below the surface or in its adjacent sea. Philpott (2003) himself highlights that while territoriality is almost completely taken for granted in its association with sovereignty, other principles were used in the past to delineate sovereignty, such as family, kinship, religion, tribe, and feudal ties. The territorial understanding of sovereignty—what we call in this article as *State Sovereignty*—is foremost grounded in a history of modern European politics valuing territorial landlordship and ownership.

The concept of sovereignty has been problematized and criticized in different ways. Authors have argued that with global interdependence, it is difficult to maintain an absolutist perspective on sovereignty (Bhandar, 2011; Havercroft, 2011). The sovereign authority might be limited in scope by international or regional treaties, by multinational corporations, or by planetary challenges such as climate change, global pandemics, or in our case, the emergence of global telecommunication infrastructures and the Internet. Other authors note that while in the classical theory it was the absolute aim of a nation (and of nationalism) to create a sovereign state (thus the “nation-state”), this goal has become more complex today, as many small nations “without states” are claiming some partial forms of sovereignty. This is what Appadurai (1990: 304) called the “disjunctive

relationship between nation and state” that is characteristic of the contemporary global situation, where a plurality of collective identities are claiming nationhood and developing political projects within or beyond existing nation-states. This is the case, for instance, of political entities where “state-sovereignty” is claimed by a significant portion of the population but also refers to domains of power within their own jurisdictions. In the case of indigenous nations, they can have the status of a government over a territory (such as the Nunavik and Nunavut Governments) or assert their nationhood to participate in decision processes concerning their recognized or claimed territories and resources.

The notion of sovereignty has also been criticized from indigenous perspectives. Coulthard (2014) argues that the peaceful coexistence of indigenous nations within settler states reproduces the colonialist, racist, and patriarchal system that subjugated them in the first place. He states that indigenous understanding of nationhood questions both “the legitimacy of the settler state’s claim to sovereignty over Indigenous people and their territories on the one hand, and the normative status of the state-form as an appropriate mode of governance on the other” (Coulthard, 2014: 36). In a recent issue of *Cultural Anthropology* dedicated to sovereignty, Bonilla (2017) argues that the political category of sovereignty is associated with violence and inequity and that, through the doctrine of *terra nullius*, was used to claim lands of so-called unsovereign, indigenous peoples. Although the concept would later be used and claimed by anti-colonial movements, Bonilla (2017) reminds us that the category itself is not neutral and that the material practice of dispossession is encoded in the rigid contemporary framework of international relations and in turn embedded in the very notion of sovereignty. For our analysis, this raises the question of knowledge production: who defines technological sovereignty and related concepts and for which purposes?

The notion has been (re)framed in directions that break from earlier understandings and which has an impact on the diverse ways in which digital/technological sovereignty is conceptualized. “Food sovereignty,” for instance, was coined in 1996 by Via Campesina and later defined as “the right of peoples to healthy and culturally appropriate food produced through ecologically sound and sustainable methods, and their right to define their own food and agriculture systems” (Declaration of Nyéléni, 2007). As described later, “food sovereignty” has inspired digital activists to assert collective or individual control over their technologies. “Body sovereignty” has also been mobilized by activists and scholars to reclaim the right to one’s body. Murphy (2012), for instance, discusses how (mostly white) feminists in the 1970s claimed sovereignty over their bodies by using techniques of vaginal self-examination and menstrual extraction to control their fertility and know how their body worked. Moreover, Wilson (2015), an indigenous scholar, argues that “body sovereignty and gender self-determination” are crucial aspects of undoing systematic forms of oppression. Here we can see a shift of the notion of sovereignty, from a collective perspective (state, nation) to a more individual one (single person, or small group of people).

Werner and de Wilde (2001) advocate for a linguistic turn to study sovereignty as a discourse. Using J.R. Searle’s speech acts theory, they suggest apprehending the concept of sovereignty as a “specific form of legitimization” rather than as an empirical category describing a preexisting situation of absolute authority over an entity. “Sovereignty,” they write, is a “a speech act to (re-)establish the claimant’s position as absolute

authority, and to legitimize its exercise of power” (Werner and de Wilde 2001: 287). They note that the “sovereignty discourse” is often absent in situations where authority is uncontested, which best corresponds to the substantial definition of sovereignty. On the contrary, it is where authority is weak that the sovereignty discourse appears more strongly (Werner and de Wilde, 2001: 307). As we will describe, this is echoed in our own analysis of digital sovereignty, where we note that the sovereignty discourse is absent in the United States, which is still the Internet’s power center.

## **Five perspectives on digital sovereignty**

In the following, we present our analysis along five categories: “Cyberspace Sovereignty,” “Digital Sovereignty, Governments and States,” “Indigenous Digital Sovereignty,” “Social Movements and Digital Sovereignty,” and “Personal Digital Sovereignty.” These categories have been designed to highlight the diverse perspectives associated with the notion of “Digital Sovereignty,” and bring to the fore some of the key actors and issues that pertain to each. It is not possible, using our methodology, to evaluate the quantitative preeminence of one category over another (in terms of number of articles in each one). Indeed we feel that the significance of each one should be asserted on its own terms: while we could expect that claims of digital sovereignty from China and Russia would attract more media or academic coverage, it is harder to defend, from a normative or qualitative perspective, that indigenous sovereignty would be less important. In our analysis, we focus rather on the overall increased use of the notion and its diversity.

It is also important to note that while our article is restricted to sovereignty as it relates to the digital, similar discourses on sovereignty and technologies predate the digital framing of the current period. For instance, the Science Council of Canada (SCC), had advocated a strategy of “technological sovereignty” as early as 1967 as a means “to develop and control the technological capability to support national sovereignty” (Globerman, 1978: 43), a strategy involving, among other things, the encouragement of Canadian ownership for technological firms and local innovation. Globerman (1978: 43) considered at that time that this policy was more related to nationalism than to increased economic efficiency of the country. Similarly, another article published a few years later (Grant, 1983), this time concerning Australia, defined technological sovereignty as “the capability and the freedom to select, to generate or acquire and to apply, build upon and exploit commercial technology needed for industrial innovation” (Grant, 1983: 239). In this case, “freedom” refers to the absence of contractual or legal constraint, and “capability” means the knowledge and technological expertise to engage in such industrial innovation. As we will see, these aspects—freedom, capacity, nationalism—are still persistent today in discourses on digital sovereignty, with an added and much stronger emphasis on the control of data.

### ***Cyberspace sovereignty***

Our first category of discourse concerning sovereignty and the digital goes back to the 1990s but is still significant today. It affirms that the regulation of the Internet extends beyond national borders and thus beyond state sovereignty. This discourse is best

exemplified by the famous manifesto entitled *A Declaration of the Independence of Cyberspace*, written in 1996 by John Perry Barlow. Let us recall here the first few sentences of this document:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather (Barlow, 1996).

This manifesto advanced the idea that the Internet was a specific space—a cyberspace—that emerged without any governmental regulations and that it should stay independent from governmental sovereignty and interventions. The manifesto was framed as a response to the efforts of governments to assert their power and authority on the digital realms, and more specifically to the Communications Decency Act of 1996 in the United States, which aimed at regulating pornography and obscenity on the Internet (Barlow, 1996; Turner, 2006: 172). In this context, cyberspace sovereignty is articulated as an opposition to state sovereignty. As we will see later, it is a very different argument than the one forcefully articulated by China and Russia for a form of Internet sovereignty or the multistakeholder stance over the Internet. Claims of “cyberspace sovereignty” were criticized at the time, notably by Wu (1997) who noted that this sovereignty was actually limited by the capacity of states to control the physical components required for Internet access. Wu (1997) argued nonetheless for a “minimally sovereign cyberspace” (p. 665) based on a consensus around widely accepted Internet standards and norms.

Although not exactly in the same framing, ideas related to cyberspace sovereignty are still present today. In a recent essay, Mueller (2017) develops the idea of “Popular Sovereignty in Cyberspace,” where he argues that the primary agents of sovereignty in cyberspace should be the people who live in cyberspace, rather than the nation-state. More specifically, Mueller argues that “multistakeholder participation,” as it is currently practiced in Internet Governance Forums (IGF) and organizations (such as the Internet Corporation for Assigned Names and Numbers [ICANN]), should be the basis of popular sovereignty on the Internet. Mueller’s essay is obviously far longer and more complex than Barlow’s manifesto. However, they both challenge state sovereignty over the Internet. Mueller (2017: ch. 5) writes that multistakeholder institutions “are a substitute for national governments and thus in some respects they pose a direct challenge to the state’s claim to supreme authority over public policy in communication and information.”

Other contemporary analyzes and writings lie in continuity with this idea that the governance of digital networks extends or should extend beyond state sovereignty. In *The Stack: On Software and Sovereignty*, Bratton (2015) develops a conceptual analysis of the relationship between software and sovereignty where he describes that the planetary-scale infrastructures of computation—which he calls “The Stack”—represents a break with the ways in which Westphalian nation-states sovereignty is enacted. Whereas the Westphalian system can be understood as creating a horizontal relationship among territorially bounded nation-states, The Stack provides a new global governing logic through which sovereignty operates. For instance, he shows how a war almost erupted

when Google Maps slightly shifted the digital representation of the border between Nicaragua and Costa Rica in 2010 (Bratton, 2015: 120).

### *Digital sovereignty, governments, and states*

Hu (2015) argues that while the Internet and transnational communication networks were perceived in the 1990s as extending beyond state sovereignty, this perspective is changing with the emergence of “the cloud” as it “indexes a reemergence of sovereign power within the realm of data” (Hu, 2015: xiii). Digital sovereignty and related terms are indeed much talked about today by states and governments. Other arguments relate more to the control of the flow of data by states.

An early reflection published in 2012 by French businessman Pierre Bellanger (2012) defined *digital sovereignty* (*souveraineté numérique*) as “the control of our present and of our destiny as they manifest and orient themselves through the use of technologies and computer networks” (p. 154, our translation). Bellanger then lamented France’s and Europe’s lack of control and independence over the evolution of digital networks and argued the need for Europe to create an economical and juridical context favoring technological innovation within its territory. This discourse is similar to the more nationalist “technological sovereignty” argument of 1970s and 1980s that we presented above, in the sense that its goal is to promote the development of national industries and local capacity for innovation. However, Bellanger also argues for digital sovereignty as a way to counter the vast “exportation of private life” of European citizens and proposes the development of national clouds on which state and citizen data should be stored. This line of argument aligns with many contemporary claims that states should assert their control over their data and telecommunication networks vis-à-vis foreign countries, especially the United States.<sup>2</sup>

Indeed, many governments have attempted to protect the state and its citizens by enacting laws and developing “national” or domestic technologies. In Brazil, then president Rousseff proposed a plan to remove the Brazilian Internet from the influence of the United States and its tech giants, characterized by some as a way to assert digital sovereignty (Rhodes and Armijo, 2014). This is also the case of Germany’s recent effort to counter the United States’ surveillance of Merkel’s phone and email conversations by building national emails, new undersea cables, and localized data storage (Maurer et al., 2015). France has also invested funds in developing governmental open source encrypted chat following the hacking of its data during the 2017 election, which some authors characterized as a desire to affirm its *souveraineté technologique* (Bergounhoux, 2018). In Canada, Obar and Clement (2013) have called for a reassertion of Canadian Network Sovereignty by improving infrastructures in order to diminish data routing through the United States. They note that national sovereignty is threatened “when an otherwise internationally independent state has its rights and powers of internal regulation and control violated by the encroachment of a foreign body” (Obar and Clement, 2013: 1).

The term *Data Sovereignty* is also of significance. Polatin-Reuben and Wright (2014) argue that this “catch-all term” has become an important subject of international debate following Edward Snowden’s public disclosures of intelligence documents in the United



States. The authors define data sovereignty as “the attempt by nation-states to subject data flows to national jurisdictions” (Polatin-Reuben and Wright, 2014: 1). They distinguish between *weak* sovereignty and *strong* sovereignty where weak sovereignty refers to “private sector-led data protection initiatives with an emphasis on the digital-rights aspects of data sovereignty” (Polatin-Reuben and Wright, 2014: 1) and strong sovereignty refers to “a state-led approach with an emphasis on safeguarding national security” (Polatin-Reuben and Wright, 2014: 1).<sup>3</sup> Analyzing the Brazil, Russia, India, China, and South Africa (BRICS) countries’ approaches toward data sovereignty, they identify Brazil, India, and South Africa as adopting a weak sovereignty approach while China and Russia as favoring a stronger sovereignty approach. The authors argue that while strong sovereignty can lead to Internet balkanization (the fragmentation of the Internet in different self-contained networks), it is also difficult to enforce and can have negative economic and political impacts, caused by a country’s isolation in digital and physical spaces. Examining the case of Indonesia, Nugraha and Sastrosubroto (2015: 465) define the notion as the “reasonable efforts by nation-states to subject national sensitive data flows to and across national borders.” They note that while “data sovereignty” is not explicitly used in Indonesian legislation, many aspects refer to these principles, such as “encryption, national email services, data center localization, national routing of Internet traffic, and national backbone communications infrastructure” (Nugraha and Sastrosubroto, 2015: 465).

We observe that discourses positively using the notion of sovereignty come from outside the United States.<sup>4</sup> Within the United States, digital sovereignty (or related terms) usually have negative connotations across the political spectrum. For instance, an article published by the Rand Corporation (Harold et al., 2016) opposes the idea of “cyber sovereignty”—which it analyzed as being claimed by China to restrict access and content on the Internet to its population—to the idea of nonrestricted and open Internet, generally attributed to United States’ perspective. This antagonism between China and Western governments has also been documented elsewhere. Using a political economy perspective, Powers and Jablonski (2015) contrast the discourses of “information sovereignty”—notably held by China—and “internet freedom”—held by Western governments—and argue that both serve to legitimize a particular political economy of globalism, the first disproportionately beneficial to Western economies, and the other supporting state efforts to control information networks (Powers and Jablonski, 2015: 203). In a similar analysis, Budnitsky and Jia (2018) argue that Russia and China have been promoting a narrative of Internet Sovereignty since 1998, as a way to counterbalance the *Internet Freedom* narrative of the Americans. For Budnitsky and Jia (2018) this narrative of “internet sovereignty” is not only an expression of digital policy but also acts as a practice of “nation branding” aiming at promoting their national identity as great powers on the international level. Budnitsky and Jia (2018) show that as was the case of the use of the notion of “technological sovereignty” in the 1970s, the current discourse on state digital sovereignty goes beyond the strictly quasi-legal definition related to the authority of a state over its territory and rather acts as a form of nationalism consisting at promoting a distinct national identity or national vision of what the Internet should be.

### *Indigenous digital sovereignty*

The notion of sovereignty is also mobilized by indigenous scholars and from an indigenous perspective, in a way that is situated in the larger struggle of indigenous peoples to reclaim sovereignty over their land, body, and culture. In an edited collection entitled *Indigenous Data Sovereignty: Toward an Agenda*, Kukutai and Taylor (2016) reflect on what data sovereignty implies for indigenous peoples. They argue that since data sovereignty “has been dominated by national governments and multinational corporations” (Kukutai and Taylor, 2016: 2), the voices and rights of indigenous peoples in relation to the “collection, ownership and application of data about their people, lifeways and territories” (Kukutai and Taylor, 2016: 2) are missing. The book showcases case studies of practices and aspirations rooted in the self-determination of indigenous peoples in the realm of digital data. For instance, in one of the chapters, Walter (2016) argues that a form of indigenous data sovereignty would mean using indigenous methodological frameworks—data collection methods not rooted in histories of colonialism—as a way to change the representation of indigenous peoples and ultimately policy making. Another chapter, written by the First Nations Information Governance Center (2016), traces the emergence and meaning attached to the concept of indigenous data sovereignty in Canada. Following the gap in data collection on reserves, a process that stemmed from indigenous peoples was initiated. As part of a Regional Health Survey, indigenous peoples spearheaded and registered the trademark OCAP®, which means ownership, control, access, and possession. This was a way for First Nations to own their information in “the same way that jurisdiction is exercised over First Nations’ lands” (First Nations Information Governance Center, 2016: 142). The issue of jurisdiction over territory and information are thus articulated through the prism of sovereignty.

In a similar vein, the book *Network Sovereignty: Building the Internet Across Indian Country* (Duarte, 2017) examines the question of the relationship between information, communication technologies (ICTs) and Indigenous people in the United States. The author writes that “[f]or tribes, sovereignty refers to the integrity of a people, as well as the integrity of their government” (Duarte, 2017: 38), a distinction made by the fact that many indigenous peoples currently live in an “imposed or negotiated colonial form of government” (Duarte, 2017: 38), that differs from what has been or could be indigenous modes of self-governance. She also distinguishes between cultural sovereignty and legal-political sovereignty and argues that the sharing of information and cultural production is integral to the exercise of sovereignty by indigenous peoples. This in turn is a way of reinforcing the knowledge of their homeland, philosophies, languages, and cosmologies (Duarte, 2017: 37). While indigenous people need to use ICTs to advance their quest for self-determination and self-governance, Duarte shows that the state of connectivity and access to different types of technologies on reserves is low. She speaks, for instance, of the lack of cellular signal on reserves, the lack of indigenous content and language on radio, and the difficulty in accessing broadband Internet, among many others. All and all, Duarte insists on the importance of technological infrastructures for indigenous resurgence, sovereignty, and self-determination.

### *Social movements and digital sovereignty*

The category “Social Movements and Technological Sovereignty” is in sharp contrast if not in rupture with claims by the states of sovereignty over the digital. It is used to affirm the autonomy of social movements through collective (and sometimes individual) control of technologies and digital infrastructures and especially their power to develop and use tools which have been designed by them and/or for them. In particular, this notion of “technological sovereignty” generally involves the use of free and open source software and services.

As we have stated in the beginning of this article, it is through the social movements’ perspective on technological sovereignty that we have decided to explore the multiple uses of the notion of sovereignty, as related to the digital. While participating in some events related to media and tech activism, this notion was presented as a way for social movements to address technological issues. Of significant importance for our work is a two-volume edited collection funded by the French civil society organization Ritimo and coordinated by researcher-activist Alex Haché (2014a, 2014b, 2017) called “Technological Sovereignty.” In her work, Haché (2014a) writes that technological sovereignty relates to “technologies developed from and for civil society” (p. 11, our translation). Civil society—sometimes used interchangeably with social movements—is defined by Haché (2014a) as citizens or collectives whose actions “are not foremost motivated by the lure of gain, but rather to respond to desires and needs and at the same time, develop social and political transformation” (p. 10, our translation).

More specifically, Haché refers to technological sovereignty as initiatives that create alternatives to commercial and/or military technologies. She puts a great emphasis on the free (and open source) software and hardware that form the basis of technological sovereignty, which should also encompass the whole life cycle of a technology, from resource extraction to disposal, as well as its sustainability, and the social norms and imaginaries surrounding it (Haché, 2014a). Activist initiatives such as decentralized community networks, encryption software, hackerspaces or activist collectives are noted in her work.<sup>5</sup> To illustrate her point, Haché refers to the metaphor of “food sovereignty” as a reference point to understand technological sovereignty. Like the concept of food sovereignty, Haché’s concept of technological sovereignty is also politically oriented: it valorizes local economies, sustainable technologies, and the right of people to control their technological systems. Drawing on Haché’s work, Beltrán (2016) characterizes technological sovereignty in a similar way as an alternative emancipation practice which she calls to promote “as an anti-establishment practice in the field of IT, in order to integrate it in other anti-imperialist struggles” (Beltrán, 2016: 18).

Another French edited collection also espouses a social movement’s interpretation of technological sovereignty. The publication, entitled *Numérique: Reprendre le contrôle* (“Digital: Regain Control”), characterizes the use and ownership of personal data by tech companies as a form of dispossession, thus highlighting the well-known fact that the data that we produce using corporate digital services like Facebook, Google, and the like, do not belong to us but rather belongs to the company who provides the service. The author (Nitot, 2016) argues that thinking about technological sovereignty can pave the way to the emergence of new practices, which will in turn change, he believes, the relationship

we have to the digital, and our control over it. To be sovereign over one's personal data is to gain in autonomy and freedom (Nitot, 2016: 3).

At the level of discourse, Nitot notes that it is not easy to convince people of the relevance of the notion of technological sovereignty. The publication argues that raising awareness is part of what technological sovereignty means and that an understanding of the current digital condition and its materiality will help the user to appropriate their technologies, data, and content. For instance, the publication proposes to use the term *privacy by using*, rather than *privacy by design* in the context of technological sovereignty to insist on the necessity to protect oneself from forms of dispossession instead of completely rejecting a technology or service provided by tech giants. The publication ends with a strong belief that users are ready for a new discourse that rethinks the current digital ecology. They argue that with the power of tech corporations, nation-states are no longer able to maintain their citizens' online safety and security, which means that the onus now resides on the latter to build their own digital sovereignty.

It is easy to see how social movement's technological sovereignty can contradict the state-oriented perspective on digital sovereignty. Although one can imagine that in a liberal democracy, the interest of civil society and the interest of the state can align in principle, this is far from being the case in authoritarian regimes. But even in so-called liberal democracies, we now know the inclinations—if sometimes covert—of governments toward mass surveillance. Indeed, in the volumes on “technological sovereignty” from a social movement perspective, the authors repeatedly mention the need to resist the stranglehold on the Internet by state or commercial powers. In these publications, the use of encryption technologies and self-managed servers are constantly framed as a way to protect “ourselves” (meaning members of those social movements) against state surveillance. In those publications, there are, however, a few blind spots among which are: the fact that people such as indigenous people and people from the global south were and are still denied forms of sovereignty, technological or otherwise, and the fact that people of color and Muslims in particular have been under surveillance for much longer than white people (see Browne, 2015).

### **“Personal” digital sovereignty**

As compared to our previous category, we want to highlight a shift from the collective to the individual. Whereas state sovereignty relates to a collective structure, the use of sovereignty may refer to an abstract “we” of civil society, while it can also relate to the individual such as the one that can be called upon to use free and open source software or encryption technologies to protect oneself. This observation brings us to our last category “Personal Technological Sovereignty” in relation to individual personhood.

Personal technological sovereignty refers to the control of an individual over their data, device, software, hardware, and other technologies. This partly echoes some writings presented in the previous section about social movements, when emphasis is made on the agency of individuals to control their technologies (for instance, by using free or open source software or encryption technologies).

The notion of individual or personal technological sovereignty can also refer to the feminist discourse about women's body sovereignty that we presented in the first section.

This association aims at trying to draw a parallel between one's body and one's technology. In her article, *Sexting Girls: Technological Sovereignty and the Digital*, Gill-Peterson (2015) refers to the relationship between technology (in this case, cell phones) and the possibility for girls to have bodily sovereignty in the sense that they can decide to engage in the practice of sexting (i.e. sending sexual selfies of themselves through this medium). While the article highlights the contradictions that emerge with this practice, it also discusses a new reading of sexting, one that instead of rendering girls as victims and in need of protection from the law, focuses on their agency, which is thought through the technological sovereignty of their bodies. While the essay questions the notion of digital sovereignty through this practice and advances the nonsovereignty of the girl who sexts, it also recognizes the trap of a binary understanding of the sovereignty of girls over their sexuality when the question is framed as either vulnerability or agency.

### **Digital sovereignty: commonalities and differences**

Our study shows that, while the term “technological sovereignty” has been used since at least the mid-1970s, there has been a recent increase in interest in the notion of “sovereignty” since 2011. In the following, we have identified a number of commonalities and differences that exist between the uses and interpretations of the notion in relation to the digital.

First, while the notion was and is still mainly used to address state control over technology, it is now being appropriated by civil society organizations, indigenous peoples, and even individuals. In a sense, we see a shift from the collective—the state as its typical expression—to the individual.

Second, the concept of technological sovereignty seems in general to relate to ideas of independence, control, and autonomy in two broad ways: (1) The capacity for collectivities (states, communities, social movements, etc.) to innovate and/or engage in technological development (for instance by stimulating national innovation for economic forms of nationalism in the case of state or developing free software or autonomous infrastructures for civil society organizations). (2) The security and/or privacy of individuals or collectives, and in relation to the ownership and control over data related to oneself, citizens, or a state.

Third, the use of “sovereignty” also has rhetorical performativity. In particular, it seems to be used to mark an opposition to different kinds of hegemonies, be it the hegemony of the United States in the interstate system (economic domination, vision of the Internet, etc.), the hegemony of corporations, or the hegemony of settlers in settler-colonial societies (in relation to indigenous claims). This echoes the analysis made by Werner and de Wilde (2001) that we presented earlier, that the sovereignty discourse appears more strongly in situations in which the authority over an entity is weaker than established. In many cases, technological sovereignty is framed as an opposition to the dominance of the United States over the Internet, and in more contemporary work, to the power of its biggest private tech companies, like Google, Amazon, Facebook, Apple, and Microsoft (sometime referred as the GAFAM). This rhetorical dimension of digital sovereignty is particularly evident in the case of China and Russia that, as Budnitsky and Jia

(2018) argue, use it as a form of nation branding to promote their own vision of Internet governance.

Fourth, and in relation to the previous point: In many cases, technological sovereignty seems to be used to conceptualize forms of counter-dominant or alternative perspectives. We note, however, that discourses of digital sovereignty do not seem to be used within the United States, except in those discourses we characterized as part of the sovereignty of cyberspace, and in the very recent case of Bannon's conservative populist use of the term. For instance, while the hacker and free software movements are very active in the United States, they do not seem (yet) to use the concept of digital sovereignty in contrast to some of their counterparts in Europe. It is, however, important to note that the US government, and especially US companies still hold great power on the Internet and the reticence of many countries to regulate them brings out the question: why do not they articulate what they do from a digital sovereignty standpoint?

Beyond these commonalities, the notion has been used in very different, if not diverging, ways. For instance, while China uses the trope of sovereignty to assert its legitimacy to control and censor data on its network, social movements use the term to protect themselves against state and commercial surveillance. We also observe that indigenous sensibilities concerning the colonial or the settler-colonial question are not necessarily shared among actors. For instance, we could expect progressive social movements to integrate such an analysis to broaden their understanding of the notion of sovereignty. But as of now, this is absent from their stance.

One question that remains open relates to the relationship between different terms. We could take for granted, for instance, that "data sovereignty" is more related to data and content rather than infrastructure (though these two dimensions are strongly related). But why, for instance, use "technological sovereignty" instead of "digital sovereignty" or "Internet sovereignty?" This could be a matter of different linguistic and cultural contexts from which these respective discourses emerge (French vs English, for instance). It might also signify an insistence on different aspects of the problem, for instance, locally situated hardware practices in the case of "technological sovereignty," or global politics in the case of "Internet sovereignty." These are, however, just hypotheses that would need to be further explored in future works.

## **Conclusion: unsettling digital sovereignty?**

The notion of "sovereignty" in relation to such terms as "digital," "data," and "technology" has increasingly been used by diverse actors to promote different perspectives. This interest for digital sovereignty (and related terms) can in part be attributed to such factors as the growing significance of the cloud (Hu, 2015) and the Snowden revelations (Polatin-Reuben and Wright, 2014), which highlighted mass surveillance and data collection by the US government and companies. The increasing use of sovereignty in the digital also echoes Bonilla's remark of a "turn to sovereignty" in social science and humanities. For Bonilla (2017: 331), this narrative emerges out of the current intellectual and geopolitical context in which states remain powerful "in both the political system and the political imagination," despite previous discourses on the presumed blurring of borders and decline of nation-states. In the case of the digital, current uses of the notion

of sovereignty should also be situated following years of technological determinist discourses claiming the erasure of the nation-state with the emergence of the Internet and the network society. As Bonilla (2017) argues, however, sovereignty as a category (or in her terms, “as a sign”) should also be questioned: the reason being that it is rooted in the Western history of colonialism and imperialism and is still deeply encoded in the structures and discourses of international law. Therefore, we feel that from the perspective of social movements (and in some cases even indigenous struggles), it should be important to question the colonial histories or power dynamics that are being maintained or reproduced when resorting to the notion of sovereignty. While the notion itself has been criticized from different epistemological and ideological perspectives, these critiques have yet to be articulated to encompass the current “turn to sovereignty” in Internet governance and in the politics of digital technologies more broadly. While digital sovereignty might currently be trendy and somewhat useful, many of the issues discussed are usually addressed without reference to colonialism, imperialism, and a critique of sovereignty itself. So the question is then: what is to be gained and to be lost in the use of sovereignty when thinking about the digital?

### Authors' note

This work has been coordinated as part of a project directed by Stéphane Couture. Both authors have contributed equally to the writing of this article.


### Acknowledgements

We would like to thank the anonymous peer reviewers for their constructive feedback as well as all those who helped us in this project. Thanks in particular to Alex Haché for her comments and Geneviève Szczepanik for her revisions, as well as our research assistants at York University, who supported us in the different steps of our research.

### Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This paper has been produced as part of a project funded by the Social Sciences and Humanities Research Council of Canada (SSHRC) and internal funding from York University.

### ORCID iD

Stéphane Couture  <https://orcid.org/0000-0002-2588-6456>

### Notes

1. Following peer-reviews, we conducted a more systematic search on databases such as WorldCat and ProQuest. This opened many more possibilities, but it also appeared that some of the documents we initially identified—especially those related to activist publications—were missing from this more formal search.
2. In a similar way, one of the authors of this article (Couture, 2013) has insisted that the use of free and open source software by states and governments is a way of ensuring sovereignty over its informational infrastructure and less dependencies from private corporations.

3. In our understanding (the authors do not deepen their definitions), weak sovereignty would mean enforcing private sector actors so they encrypt their data and respect the privacy of their citizens, while strong sovereignty would signify that states have their own infrastructures.
4. This could be changing however. In a recent interview, Steve Bannon (former strategist of president Trump) listed “digital sovereignty” as one of three converging forces that shape the world referring here to the need for citizens to oppose “central technocratic state capitalist” (his words) companies like Google and Facebook taking away intellectual property (Barber, 2018: 8m37).
5. One reviewer wondered if the rise of the term “sovereignty” might mean a decrease in the relevance of terms such as “free” and “open” and if so, the reason for this shift. The authors that we present in this analysis do not themselves provide such justification. However, we could argue that the sovereignty discourse, while maintaining the ideals of free software, offers the promise of enlarging the focus to encompass contemporary issues like privacy and rapid obsolescence while also aligning it more explicitly with a political perspective.

## References

- Appadurai A (1990) Disjuncture and difference in the global cultural economy. *Theory, Culture & Society* 7(2–3): 295–310.
- Barber L (2018) *Steve Bannon Interview: FT future of news conference*. Available at: <https://www.youtube.com/watch?v=vO9TyxqbHTI> (accessed 24 June 2018).
- Barlow JP (1996) *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation, 8 February. Available at: <https://www.eff.org/fr/cyberspace-independence> (accessed 14 November 2017).
- Bellanger P (2012) De la souveraineté numérique. *Le Débat* 170(3): 149–159.
- Beltrán NC (2016) Technological sovereignty: what chances for alternative practices to emerge in daily IT use? *Hybrid. Revue des arts et médiations humaines*. Available at: <https://www.semanticscholar.org/paper/Technological-Sovereignty%3A-What-Chances-for-to-in-Beltran/b26e0d1f1c21497b2980f8515d6ce7948d9c892f>
- Bergounhoux J (2018) Pourquoi le gouvernement Macron se dote de sa propre messagerie sécurisée. *Usine-digitale.fr*, 18 April. Available at: <https://www.usine-digitale.fr/article/pourquoi-le-gouvernement-macron-se-dote-de-sa-propre-application-de-chat-securisee.N682094> (accessed 22 June 2018)
- Bhandar B (2011) The conceit of sovereignty: toward post-colonial technique. In: Lessard B (ed.) *Stories Communities: Narratives of Contact and Arrival in Constituting Political Community*. Vancouver, BC, Canada: University of British Columbia Press, pp. 66–88.
- Bonilla Y (2017) Unsettling sovereignty. *Cultural Anthropology* 32(3): 330–339.
- Bratton BH (2015) *The Stack: On Software and Sovereignty* (Software studies). Cambridge, MA: The MIT Press.
- Browne S (2015) *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.
- Budnitsky S and Jia L (2018) Branding Internet sovereignty: digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies* 21(5): 594–613.
- Coulthard SG (2014) *Red Skin, White Masks: Rejecting the Colonial Politics of Recognition*. Minneapolis, MN: University of Minnesota Press.
- Couture S (2013) Logiciels Libres: Réduction Des Coûts et Souveraineté Numérique. Note socio-économique [Free Software: Cost Reduction and Digital Sovereignty. Socio-economic note]. Montréal: Institut de recherche et d'informations socio-économiques (IRIS). Available at: <http://www.iris-recherche.qc.ca/wp-content/uploads/2013/09/Note-Logiciels-libres.pdf> (accessed 25 July 2019).



- Couture S (2018) Embedding social justice in Internet Infrastructures: sociotechnical proposals from civil society in the context of Internet Governance. In *Presentation at the Canadian Communication Association Conference* 30 May – 1 June 2018. Regina: University of Regina.
- Couture S, King G, and Toupin S, et al. (2016) “Another World Possible”? Reflections from the Media@McGill research delegation to the 2015 world social forum in Tunisia. *Canadian Journal of Communication* 41(1): 157–167.
- Duarte ME (2017) *Network Sovereignty: Building the Internet across Indian Country*. Seattle, WA: University of Washington Press.
- First Nations Information Governance Centre (2016) Pathways to First Nations’ data and information sovereignty. In: Kukutai T and Taylor J (eds) *Indigenous Data Sovereignty: Toward an Agenda* (CAEPR). Canberra, ACT, Australia: ANU Press, pp. 139–156.
- Gill-Peterson J (2015) Sexting girls: technological sovereignty and the digital. *Women & Performance* 25(2): 143–156.
- Globerman S (1978) Canadian science policy and technological sovereignty. *Canadian Public Policy/Analyse De Politiques* 4(1): 34–45.
- Grant P (1983) Technological sovereignty: forgotten factor in the “Hi-Tech” Razzamatazz. *Critical Studies in Innovation* 1(2): 239–270.
- Haché A (2014a) La souveraineté technologique. *Dossier Ritimo*. Available at: <https://www.ritimo.org/IMG/pdf/dossier-st1.pdf>
- Haché A (2014b) Technological sovereignty. *Mouvements* 79(3): 38–48.
- Haché A (2017) *Technological Sovereignty*, vol.2. Barcelona. Available at: <https://www.ritimo.org/IMG/pdf/sobtech2-en-with-covers-web-150dpi-2018-01-10.pdf>
- Harold SW, Libicki MC and Cevallos AS (2016) *Getting to Yes with China in Cyberspace*. Santa Monica, CA: Rand Corporation. Available at: [https://www.rand.org/pubs/research\\_reports/RR1335.html](https://www.rand.org/pubs/research_reports/RR1335.html) (accessed 22 June 2018).
- Havercroft J (2011) *The Captive of Sovereignty*. Cambridge, MA: Cambridge University Press.
- Hinsley FH (1986) *Sovereignty*. 2nd ed. Cambridge, MA: Cambridge University Press.
- Hollis DB (2012) *Stewardship Versus Sovereignty? International Law and the Apportionment of Cyberspace* (ID 2038523, SSRN scholarly paper, 19 March). Rochester, NY: Social Science Research Network. Available at: <https://papers.ssrn.com/abstract=2038523> (accessed 21 September 2017).
- Hu TH (2015) *A Prehistory of the Cloud*. Cambridge, MA: The MIT Press.
- Krippendorff K (1993) Major metaphors of communication and some constructivist reflections on their use. *Cybernetics & Human Knowing* 2(1): 3–25.
- Kukutai T and Taylor J (2016) *Indigenous Data Sovereignty: Toward an Agenda* (CAEPR). Canberra, ACT, Australia: ANU Press.
- Maurer T, Skierka I and Morgus R (2015) Technological sovereignty: missing the point? In: *2015 7th international conference on Cyber conflict: Architectures in cyberspace (CyCon)*, pp. 53–68. IEEE. Available at: <http://ieeexplore.ieee.org/abstract/document/7158468/> (accessed 18 September 2017).
- Mueller M (2017) *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Malden, MA: Polity.
- Murphy M (2012) *Seizing the Means of Reproduction: Entanglements of Feminism, Health, and Technoscience*. Durham, NC: Duke University Press.
- Nitot T (2016) *Numérique : reprendre le contrôle*. Paris: Framasoft. Available at: [https://frama-book.org/docs/NRC/Numerique\\_ReprendreLeControle\\_CC-By\\_impress.pdf](https://frama-book.org/docs/NRC/Numerique_ReprendreLeControle_CC-By_impress.pdf)

- Nugraha YK and Sastrosubroto AS (2015) Towards data sovereignty in cyberspace. In: *2015 3rd international conference on information and communication technology (ICoICT)*, May 2015, pp. 465–471. Available at: <https://ieeexplore.ieee.org/document/7231469>
- Obar JA and Clement A (2013) *Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty* (ID 2311792, ssrn scholarly paper, 1 July). Rochester, NY: Social Science Research Network. Available at: <https://papers.ssrn.com/abstract=2311792> (accessed 24 June 2018).
- Peters B (2016) Digital. In: Peters B (ed.) *Digital Keywords: A Vocabulary of Information Society and Culture*. Princeton, NJ: Princeton University Press, pp. 93–108.
- Philpott D (2003) Sovereignty. *Stanford Encyclopedia of Philosophy Archive*, 31 May. Available at: <https://plato.stanford.edu/archives/sum2016/entries/sovereignty/> (accessed 24 June 2018).
- Polatin-Reuben D and Wright J (2014) An Internet with BRICS characteristics: data sovereignty and the Balkanisation of the Internet. *Usenix*, 7 July. Available at: <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>
- Powers SM and Jablonski M (2015) *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana, IL: University of Illinois Press.
- Proulx S (2007) Interroger la métaphore d'une société de l'information : horizon et limites d'une utopie. *Communication & Langages* 152: 107–124.
- Rhodes SD and Armijo LE (2014) Brazilian leadership and the global Internet. *AULA Blog*. Available at: <https://aulablog.net/tag/digital-sovereignty/> (accessed 14 November 2017).
- Sélingué M (2007) Forum for food sovereignty. *Declaration of Nyéléni*, 27 February. Available at: <https://nyeleni.org/spip.php?article290> (accessed 22 June 2018).
- Toupin S (2014) Feminist hackerspaces: the synthesis of feminist and hacker cultures. *Journal of Peer Production* 5: 1–11.
- Turner F (2006) *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, IL: University of Chicago Press.
- Walter M (2016) Data politics and Indigenous representation in Australian statistics. In: Kukutai T and Taylor J (eds) *Indigenous Data Sovereignty: Toward an Agenda* (CAEPR). Canberra, ACT, Australia: ANU Press, pp. 79–98.
- Werner WG and De Wilde JH (2001) The Endurance of sovereignty. *European Journal of International Relations* 7(3): 283–313.
- Wilson A (2015) Our coming in stories: cree identity, body sovereignty and gender self-determination. *Journal of Global Indigeneity* 1: 4.
- Wu TS (1997) Cyberspace sovereignty? The Internet and the international system. *Harvard Journal of Law & Technology* 10(3): 647–666.

## Author biographies

Stéphane Couture is an assistant professor in the bilingual program in Communications at Glendon College, York University, Toronto, Canada. His research addresses the values and politics of technological design and the role of civil society in the development of Internet infrastructures.

Sophie Toupin is a PhD candidate in the Department of Art History and Communication Studies at McGill University in Montréal, Canada. Her current PhD research examines the relationship between communication technologies and revolutionary movements in the context of liberation struggles.