10

Conclusion

Digital Sovereignty in the BRICS: Structuring Self-Determination, Cybersecurity, and Control

Luca Belli and Min Jiang

10.1 INTRODUCTION: DIGITAL SOVEREIGNS OR DIGITAL SUBJECTS?

This chapter acknowledges both the fluidity and complexity of the notion of digital sovereignty, while also highlighting the necessity of digital sovereignty strategies, policies, and governance mechanisms, envisaged especially by leading emerging economies. As we discuss in the introductory chapter, digital sovereignty suffers from a lack of a consensus regarding both the substance and contours of the concept. In this regard, the analysis of various conceptualizations of this notion as well as its concrete implementations in BRICS countries allows us to move beyond the conventional, normative, state-centric approach toward "sovereignty" that dominates in Western scholarly, policy, and popular debates. Doing so also allows us to engage with how "digital sovereignty" is perceived and practiced in reality by not only nation-states but also empowered individuals, companies, indigenous populations, activist groups, and even supranational entities including the BRICS.

In this spirit, the chapter notes that digital sovereignty narratives and initiatives play a pivotal role in fostering self-determination,[1] while increasing cybersecurity capabilities and strengthening the capacity to exercise control over digital infrastructures and data of the various types of "digital sovereigns." Importantly, depending on the conception of digital sovereignty

[1] As pointed out in the introductory chapter of this volume, this work stresses the instrumental role of digital sovereignty in the achievement of the internal dimension of self-determination, that is, the right to freely determine and pursue one's economic, social, and cultural developments, including by independently choosing, developing, and adopting digital technologies. Such conception also includes the fundamental right to "informational self-determination" enshrining the individuals' faculty to exert control over their personal data, as an expression of the human right to have and develop a personality. See Chapter 1, note 1.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

that we decide to utilize and the initiatives at stake, a "digital sovereign" can be an individual, a community, a corporation, a state, or even a supranational organization.[2]

Indeed, the examples analyzed in this volume illustrate how individuals, communities, corporations, states, and supranational organizations can become digital sovereigns by understanding, developing, and regulating the use of digital technologies, according to their needs, aspirations, and values. Conversely, aspiring digital sovereigns can be turned into digital subjects when there is insufficient understanding, development, or command of such technologies even when "digital sovereignty" policies and plans are formally adopted.

As we contend along the chapters of this book, digital sovereignty is a multifaceted and contested concept. It may be considered something positive or negative, depending on who the sovereign entity is, and how the entity decides to structure its sovereignty capability. It is important to emphasize that remarkably similar policies may be aimed at defending a nation from cyberattacks or surveilling it, may strive to promote local talent, fostering the development of indigenous technologies, or blatantly enact protectionist agendas, preserving the position of cronies. Chiefly, the positive or negative assessment of this concept will strongly rely on how the construction and deployment of digital sovereignty affects the rights and agency of others. As such, the digital sovereignty label indicates the idea that digital sovereigns assert their agency, authority, and capacity to "pursue their economic, social and cultural development"[3] through the digital technologies they use. Such a vision introduces a new element of complexity, dependent on the *capability* of a sovereign entity to understand and exercise power through technology without being necessarily bound to a specific territory. These elements challenge the traditional state-centric conceptions of sovereignty, which rely on a nation-state's domestic authority and control over a given population in a specific territory and its monopoly in the definition of international legal instruments, alliances, and exercise of military power.

The concept of digital sovereignty does not obliterate the importance of the above-mentioned elements but brings to the fore the essential role of technology systems in expanding authority, self-determination, and control. In this perspective, a digital sovereign is the entity that owns, operates, and, ultimately,

[2] For instance, digital sovereignty was recognized as a priority for the European Union, which is a supranational organization. In a statement just prior to her appointment as president of the European Commission, Ursula von der Leyen, called for Europe to achieve "technological sovereignty in some critical technology areas" stating that "Europe must have (the technological capacity) to make its own choices, according to its own values, respecting its own rules" while not hiding the explicit ambition that Europe "define standards for this new generation of technologies that will become the global norm." (von der Leyen, 2020).

[3] See the definition of the fundamental right to self-determination in Article 1 of the *Charter of the United Nations* as well as in Article 1 of both the *International Covenant on Economic, Social and Cultural Rights* and the *International Covenant on Civil and Political Rights*.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

has the capacity to understand, regulate, and control the technology can and will be used. To appreciate the breath and relevance of digital sovereignty, it is therefore useful to emphasize the "structural power" of (digital) technology. The structural power concept was first elaborated by political scientist Susan Strange in *States and Markets* (1988). In her vision, power can be exercised not only through command and control and the ability to compel someone to do something by establishing regimes that regulate societies but also through the power to shape the structures defining the frameworks within which people, corporations, and states relate to each other.

Strange's conception of structural power can be seen as a sovereign entity's capability to shape the bureaucratic, commercial, or even technological "labyrinths" enabling interactions among people, organizations, businesses, and states. The sovereign defines where walls or doors will be in the labyrinth, shaping its "architecture" (Lessig, 1999a, 2006), thus ultimately exercising power by controlling and regulating the capacity of those who use the labyrinth to move and interact. In this sense, Strange's work provides a useful perspective from which we can read Lessig's concept of software and hardware architectures as regulation. Here, architectures act as constraints that can structure (cyber)spaces in both the physical[4] and digital realms, determining whether specific behaviors are allowed by design, and thus playing a regulatory function (Belli, 2022).

Awareness of the use of digital technology for surveillance or "data colonialism" (Benyera, 2021; Couldry & Mejias, 2018) has been matched by the increasing understanding of the central role played by digital technology to structure national economy, society, and governance. Hence, understanding the relevance of the structural power of technology is essential to realizing the relevance of digital sovereignty and, more broadly, the regulatory function of technology (Benyera, 2021; Couldry & Mejias, 2018). It would be either incorrect or hubristic – or both – to argue that the nation-state is the only possible digital sovereign. Indeed, individuals, communities, organizations, and businesses that understand, develop, and deploy digital technologies can all be considered digital sovereigns as they are not only regulated by technologies but also enjoy self-determination thanks to technology and may even be able to elude the implementation of traditional state sovereignty through the exercise of their digital sovereignty.

As this volume demonstrates, especially from a Global South perspective, a very large spectrum of different entities may engage in understanding, developing, and mustering digital technologies. Importantly, as we have stressed previously, the entities that manage to become digital sovereigns are not only states. Community networks built and operated by local communities are interesting examples in this regard, which can be found in several BRICS

[4] An example offered by Lessig is the architecture of the city of Paris, which was reorganized with large avenues by Baron Haussmann to prevent rebellious people from taking control of the city center, as previously happened during the third French revolution of 1848 (Lessig, 2006).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

countries. These crowd-sourced, bottom-up networks are excellent examples of entities pursuing a form of Commons Digital Sovereignty, which frequently emerges not only as a community-driven alternative to corporate and state approaches, but as a concrete strategy to cope with the limitations and failures of the traditional public and private approaches.

Internet access infrastructures created by local communities to overcome digital divides and achieve "network self-determination"[5] illustrate that digital sovereignty can stem from the actions of empowered communities, where individuals cooperate to build technology, understand its functioning, and exert control over the local digital infrastructure, thus appropriate the benefits of tech-enabled social, economic, and cultural developments (Belli, 2017). The commons approach to digital sovereignty, with mounting evidence from several BRICS countries including Brazil, India, and South Africa, can be seen as a by-product of communities yearning for network self-determination (Belli & Hadzic, 2022; Belli & Hadzic, 2023; GISWatch, 2018). Indeed, such examples demonstrate that even vulnerable and marginalized communities such as Brazilian *quilomobola*[6] women or rural communities and slum-dwellers in South Africa and India can become the protagonists and participants of their digital futures, learning how to build and use new digital infrastructures and new services for the local communities, based on the needs and characteristics of the local communities.

Indeed, as we have demonstrated in the chapter of this volume, digital sovereignty is not only fostered by states but can also be crafted by local communities. Despite not having explicit digital sovereignty agendas, community networks offer intriguing examples of "good digital sovereignty" (Belli, 2023), illustrating how new digital architectures can be constructed, managed, and self-regulated using a bottom-up approach (Belli, 2017). They tellingly demonstrate that internet connectivity and entire digital ecosystems can be built by the local communities for the local communities, demonstrating that groups of individuals that previously were scarcely connected or totally unconnected can become digitally sovereign. Such commons-based conception of digital sovereignty can not only lead the local community to start understanding the

[5] Network self-determination is defined as the "right to freely associate in order to define, in a democratic fashion, the design, development and management of network infrastructure as a common good, so that all individuals can freely seek, impart and receive information and innovation." The concept is based on the consideration that by freely developing connectivity infrastructure, individuals and communities quintessentially enjoy their fundamental right to self-determine, that is, to "pursue their economic, social and cultural development" through the opportunities that connectivity can offer (Belli, 2017).

[6] Quilombos are communities that emerged as refuges for African enslaved individuals who escaped exploitation during the entire period of slavery in Brazil, established by Portuguese colonizers in the sixteenth century and maintained until 1888. The inhabitants of these communities are called quilombolas. With the adoption of the 1988 Constitution, Brazil enshrined the quilombolas right to own and use the land they were on. Today Brazil has more than fifteen thousand quilombola communities (Zanolli, 2021, pp. 121–128).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

functioning and developing digital technology but also strive to shape their economic, social, and cultural developments (Belli, 2017; Belli & Hadzic, 2022; Belli & Hadzic, 2023; Bidwell & Jensen; 2019; GISWatch 2018).

Besides providing access to previously disconnected populations, these community networks also give rise to an ample range of positive externalities, including the construction of new infrastructure with limited investment, the engagement of locals in the development of new self-governance models, the revitalization of social interactions among local community members, and the emergence of new opportunities for accessing information, learning, doing business, and creating employment (Belli, 2017; Bidwell & Jensen, 2019).

In this perspective, these initiatives are real laboratories of digital sovereignty for local communities that experiment with digital technologies to understand their functioning, thus developing a better understanding not only of the technology itself but of the type of governance and regulation compatible with their community. It leads the local communities to develop "good digital sovereignty," thanks to their capacity to understand, develop, and regulate their local digital ecosystems, while connecting them to the global internet (Belli, 2017; Belli & Hadzic, 2023).

It becomes increasingly evident that a comprehensive plan guided by a long-term perspective is essential to the successful implementation of digital sovereignty initiatives. Those who manage to do so may have a better chance of becoming digital sovereigns, where they can avoid or minimize the risks brought by technical and economic dependence on foreign technology. Those who do not may turn into digital subjects (or digitally colonized) by other more powerful digital sovereigns. Unfortunately, the "vision" of digital sovereignty of most states often lacks farsightedness and a holistic approach to this issue.

Importantly, a variety of different goals may be explicitly or implicitly included within digital sovereignty narratives, as digital technologies and their structural power can facilitate enormous social and economic advancements but can also be weaponized against individuals, corporations, and nation-states. In such contexts, this chapter takes a more agnostic approach toward digital sovereignty, exploring a selection of practices and providing insight into what this concept means in practical terms. In this respect, BRICS countries' approaches offer some telling examples of how and why the need for digital sovereignty can emerge as well as how confused, contradictory, and even dysfunctional the implementation of policies aiming at digital sovereignty can be.

10.2 THE EMERGENCE OF THE DIGITAL SOVEREIGNTY DISCOURSE IN THE BRICS

The heterogeneity, cultural richness, and historical backgrounds of the BRICS are also reflected in their diverse approaches to digital sovereignty. The differences in their state digital sovereignty strategies can be partly explained by their divergent political stances.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

As noted by Johannes Thumfart's contribution in this volume, Russia and China, and to a lesser extent India, have traditionally played an antagonistic role to the digital superpower, the US, and have structured their approaches to digital sovereignty based on such antagonism. Their clear intention to avoid reliance on US technology is a decades-long strategic choice. Historically, the RIC[7] countries have not only had a strongly suspicious and frequently confrontational attitude toward the US but also associated dependence on US technology with high risks.

A telling example is the existence of alternatives to the Global Positioning Systems (GPS), which was established by the US in the late 1970s. GPS, an essential component of a wide range of digital products and services, plays a critical role for many for military technologies used for defense purposes. Out of the five alternatives to the dominant US system, the first three were developed by Russia, China, and India.[8] The EU and Japan have also decided to create alternative systems in recent years as they become increasingly mindful of how critical it is to be strategically autonomous.[9]

India, Brazil, and South Africa have also strong historical reasons for being particularly attached to their (digital) sovereignty. These span from postcolonial resentments against imperialist attitudes of old colonizers, feeding several decades-long engagements in "South-South cooperation" (The South Commission, 1990)[10] through numerous initiatives, such as the Group of 77, the Non-Aligned Movement and Group of 15, the IBSA Trilateral[11] and,

[7] The RIC Trilateral Alignment was established by Russia, India, and China in 2001 (O'Donnell & Papa, 2021).

The RIC Trilateral Alignment is not the only official club created by BRICS countries before the BRICS: in 2003, India also cofounded the IBSA Trilateral, together with Brazil and South Africa (see note 212, below), and in 2017, India also joined the Shanghai Cooperation Organization (SCO), a larger alignment that also includes China and Russia.

[8] The Global Navigation Satellite System (GLONASS) was developed by Russia in the 1980s; China started the development of the BeiDou Navigation Satellite System (BDS) in the 2000s; India launched the development of the Navigation with Indian Constellation (NavIC) in the 2010s.

[9] The EU Galileo system and the Quasi-Zenith Satellite System (QZSS) led by Japan were developed since 2015.

[10] Already in 1990, the seminal Report of the South Commission called for South-South cooperation, emphasizing that "the emerging development patterns of the North clearly suggest that the Northern locomotive economies will not pull the train of Southern economies at a pace that will satisfy its passengers – the people of the South. The locomotive power has to be generated to the maximum extent possible within the economies of the South themselves." (The South Commission, 1990, p. 286). The South Commission, formally established in 1987, fostered discussions among intellectual and political leaders from the South and evolved into the South Centre, an intergovernmental organization established in 1995. www.southcentre.int/.

[11] Little known to the public, IBSA is a trilateral forum that brings together India, Brazil, and South Africa to foster consultation and coordination on global and regional political issues; collaboration on concrete projects; and assisting other developing countries through the IBSA Fund. See www.ibsa-trilateral.org/. This organization become well known to internet

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

finally, the BRICS grouping.[12] These countries also harbor strong sensitivities stemming from the US abuses of its dominant position in the digital realm.

Such egregious abuses have pushed the BRICS to seek alternative paths of digital development and policymaking. Notably, former NSA contractor Edward Snowden revealed the Brazilian head of state Dilma Rousseff herself was personally a victim of illegal wiretapping (MacAskill & Dance, 2013). Such an episode represented a true wake-up call for the BRICS grouping. Indeed, post-Snowden, BRICS nations have been reorganizing their postures to enhance their cooperation on digital matters – especially in cybersecurity (Belli, 2021a, 2021b, 2021c) – as a reaction to the unlimited digital sovereignty exercised by the US globally.

Snowden revelations exposed the strategic risks associated with the massive use and dependence on foreign technologies. The real costs of "free services" are paid de facto by granting a license to large-scale collection of personal data as well as the consequent loss of privacy, competition, sovereignty, and informational self-determination.[13] However, it may be argued that the actor mainly responsible for the global awakening of the risks associated with the "weaponization" of digital policies was the Trump Administration that frequently targeted adversaries with several executive orders (Jiang, 2019) accompanied by bombastic announcements via social media.

Indeed, the periodic use of executive orders in prohibiting US tech firms from supplying software or hardware components to Chinese manufacturers such as ZTE and Huawei has led many governments and businesses around the world to reconsider their supply chains and grasp the importance of digital sovereignty in terms of strategic autonomy, self-sufficiency, and

governance scholars in 2011, when it put forward a proposal for a UN Committee for Internet-Related Policies, which was strongly contested at that year's UN Internet Governance Forum and, despite the contestations, endorsed by the Indian Government at the 66th Session of the UN General Assembly in October 2011 (Belli, 2011).

[12] The G77 was established in 1964 as a developing countries' interest group. G15 emerged within the Non-Aligned Movement in 1989. The IBSA Trilateral was created in 2003. BRICS was formed in 2009. They have all been considered "locomotives of the South" defined by the Report of the South Commission, raising hopes of an alternative to the world order imposed by the Global North. A compelling review of how and why such groupings were created as well as the subsequent South-South cooperation attempts is provided by V. Prashad in "Poorer Nations: A Possible History of the Global South" (2012).

[13] Since the early 1980s, the fundamental right to "informational self-determination" has become a cornerstone of personal-data protection, starting to be consecrated as an expression of the right to free development of the personality. Particularly, in 1983, the landmark "Census" decision of the Federal Supreme Court of Germany (1983) stressed that the right to informational self-determination underpins "the capacity of the individual to determine the disclosure and use of his/her personal data," thus ascribing to individuals the right to choose what personal data about themselves can be disclosed, to whom, and for what purposes such data can be used. The principle is considered to be a cornerstone of modern data protection and is explicitly enshrined by art. 2 of the Brazilian General Data Protection Law as one of the founding elements of the Brazilian data protection framework (CyberBRICS, 2020).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

self-determination.[14] While such concerns have been particularly acutely felt among BRICS countries, many Western countries shared them as well, especially at the EU level (von der Leyen, 2020).

Recent years have witnessed the considerable transformation of the perception of digital sovereignty from an initial negative connotation associated with authoritarian ambition to a more positive conceptualization for recognizing its relevance in community, national, and international agendas. A growing chain of events has shown there are concrete risks associated with the inability to exercise digital sovereignty, thus being subject to the unilateral decisions of those able to assert agency, power, and control over digital infrastructure, data, services, and protocols. Indeed, the notion of digital sovereignty gradually progressed from a niche concept, primarily supported by China and few other developing countries, and frequently purported as an autocratic cliché, to a mainstream issue now advocated by EU leaders as an essential tussle to reassert strategic autonomy.

10.3 RESISTING FOREIGN ESPIONAGE, MEDDLING, AND SANCTIONS

We must note that the various initiatives that emerged over the past decade in the BRICS countries and beyond to pursue digital sovereignty have not been merely motivated by a mere desire to avoid US espionage. On the contrary, the increasing awareness of the US's invasive behaviors through its technological apparatus has led BRICS countries to realize that without alternatives, their technological disadvantage would have led to irreversible economic dependence and ultimately (digital) colonization.

First, on top of fearing being victim of weaponized digital policies, countries around the world understand that the main concerns raised by Edward Snowden in 2013 remain substantially unchanged. In July 2020, the European Court of Justice (ECJ) in its Schrems II case invalidated the Trans-Atlantic transfer of personal data from the EU to the US due to the nature of US government access to data held by American corporations under existing intelligence activities. Particularly the Court held that such activities undermine "the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary" (*Data Protection Commissioner* v *Facebook Ireland Ltd*, 2020, para 184).

To understand why the digital sovereignty sentiments have been growing globally, motivated by mistrust toward dominant US technologies, it is instructive to consider the normative analysis of the ECJ. Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorizes the collection, use, and

[14] See the first chapter of this book but also the detailed analysis offered by A. Chander and H. Sun (2022).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

dissemination of electronic communications content stored by US platforms (such as Facebook, Google, and Microsoft) or transported across the internet's "backbone" infrastructure, thus compelling US connectivity providers (such as AT&T and Verizon) to cooperate with national intelligence agencies (*Data Protection Commissioner* v *Facebook Ireland Ltd*, 2020, para 184).[15]

The reactions that this situation triggered in the BRICS countries are tellingly illustrated by former Brazilian President Dilma Rousseff's opening remarks at 68th UN General Assembly, describing the NSA scandal in the following terms:

> As many other Latin Americans, I fought against authoritarianism and censorship, and I cannot but defend, in an uncompromising fashion, the right to privacy of individuals and the **sovereignty of my country**.
>
> In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy. In the absence of the **respect for sovereignty**, there is no basis for the relationship among Nations.
>
> We face, Mr. President, a situation of grave violation of human rights and of civil liberties; of invasion and capture of confidential information concerning corporate activities, and especially of **disrespect to national sovereignty**. (Rousseff, 2013) [emphasis added]

It is in this context that BRICS countries have started some of their most ambitious initiatives aimed at reasserting digital sovereignty, both independently and as a grouping. Since the BRICS Summit issued the *2013 eThekwini Declaration and Action Plan* in Durban, South Africa, BRICS nations have made explicit their desire to enhance their cooperation on cybersecurity, expressing for the first time their desire "to contribute to and participate in a peaceful, secure, and open cyberspace" while calling for the elaboration of "universally accepted norms, standards and practices" (BRICS, 2013). Consequently, BRICS leaders established the "Working Group of Experts of the BRICS States on security in the use of ICTs" with a mandate to, inter alia, "develop practical cooperation with each other in order to address common security challenges in the use of ICTs" (BRICS, 2015).

Individual initiatives also followed suit as the governance, regulation, and development of digital technologies have swiftly gained prominence in each BRICS country's agenda. In 2014, Brazil approved its Internet Rights Framework (Marco Civil da Internet) to regulate *inter alia* data protection in the online environment and agreed to start the construction together with the EU of EllaLink,[16] a new submarine fiber-optic cable. This cable connects Seixas, Portugal directly with Fortaleza, Brazil without having to pass through Miami, US, where all previous submarine cable landed as part of US telecom backbone. The inauguration of EllaLink in June 2021, after several years of

[15] See notably the ECJ considerations on the PRISM and UPSTREAM surveillance programs, regulated by Section 702 of the FISA and Executive Order 12333.

[16] For more information about EllaLink, see https://ella.link.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

development, is an example of an infrastructure initiative aimed at strengthening digital sovereignty to enhance strategic autonomy from US technology while reducing dependency on US suppliers.

The considerable time and financial cost of the initiative, however, are also a stark reminder of how complex it is to build such strategic autonomy, how necessary it is to adopt a systemic long-term plan, and how difficult it is to maintain a particular digital sovereignty stance in an unstable geopolitical environment. Understanding how digital technologies works, crafting a sound and comprehensive strategy to frame their governance, securing adequate resources to implement such a strategy, and having a stable environment to avoid disruption are key elements in implementing digital sovereignty, be it exercised by individuals, communities, corporations, states, or supranational entities. Such elements are much easier to crystallize in countries that enjoy strong political stability and a systemic approach to technology, while they are much rarer in countries where administrations lack technological understanding and subsequently hold radically different – or frequently contradictory – postures toward digital sovereignty.

Within BRICS, China is clearly a country enjoying relative political stability, systematic governance, and deployment of digital technologies. However, even the presence of these elements does not guarantee the achievement of digital sovereignty without a long-term plan. For example, in Russia, the regulation of internet infrastructure and calls for cyber sovereignty started to appear as early as the 2010s. Since then, a number of initiatives have been gradually implemented over the subsequent decade with the goal of achieving digital self-sufficiency and enhancing the country's digital cyber-control, cyber-defense, and offense capabilities. Importantly, Russia, China, and other members of the Shanghai Cooperation Organization (SCO) released the first version of their International Code of Conduct for Information Security, updated in 2015, stressing that "policy authority for Internet-related public policy issues is the sovereign right of States." (Ministry of Digital Development, Communications and Mass Media of the Russian Federation, 2015).[17]

In 2012, Russia established a legal framework for website blocking and in 2015 introduced data localization provisions, which mandate the storage of personal data in servers located in the national territory (Shcherbovich, 2021). These policies laid the ground for the institutionalization of the "internet sovereignty" discourse, articulated by Deputy Chairman of the State Duma Irina Yarovaya and consecrated into legislation in 2019, frequently dubbed

[17] Already in 2015, Russia announced its willingness to develop a "independent" mobile operating system reduce and ideally break the iOS and Android duopoly by Apple and Google. Notably, the Russia Ministry of Telecommunications adamantly supported the use of Free and Open Software as the base "for creation of international industrial consortium for development of alternative software products […] relying on collaboration with BRICS-countries" (Ministry of Digital Development, Communications and Mass Media of the Russian Federation, 2015).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

as "Yarovaya Law" (Shcherbovich, 2021). Russia has dedicated considerable efforts to territorialize its digital infrastructure[18] and exert control over information flows in a bid to not only assert control over the national digital environment but also resist foreign cyberattacks and skirt the disruptive effects of foreign sanctions. The establishment of a national segment of the internet, known as the "RuNet," heavily reliant on the adoption of Russian hardware and software facilitates the pervasive control of information flows by Russian Internet Service Providers, while also providing strategic autonomy to a country that has massively bet on digitalization.

It is important to note that the Russian case illustrates the juxtaposition of cybersecurity, digital sovereignty, and (social) control narratives. Undeniably, the Russian government has frequently utilized the same measures that are branded as enhancing digital sovereignty to monitor Russian citizens and unduly block undesired content online.[19] As argued in this book by Olga Bronnikova and colleagues, the implementation of the various iterations of SORM (System for Operative Investigative Activities) illustrates how digital sovereignty and cybersecurity discourse may also represent a convenient way to expand national surveillance operations.

However, the Russian push for the "sovereignization of the internet" (Grover & Thomas, 2021) has been justified not only by the fear of foreign meddling exposed by Snowden revelations or the willingness to control online speech but also by the increasing need to develop a self-sufficient national network able to resist the disruption of foreign sanctions and mitigate foreign cyberattacks on national digital infrastructure as seen in Russia's ongoing war in Ukraine. For instance, in June 2019, the *New York Times* reported that the US Cyber Command was stepping up its "digital incursions" into Russia's electric power grid in accordance with the Command's attributions to "conduct clandestine military activity to deter, safeguard or defend against attacks" (Sanger & Perlroth, 2019).

Concrete initiatives aimed at constructing digital sovereignty in Russia have emerged partly out of the need for survival. This is the case of Mir,[20] a Russian

[18] Here the term "digital infrastructure" should be considered as any physical and logical asset, that is, not only the physical infrastructure aimed at providing connectivity, but also the protocols and applications that facilitate communications, as it is generally understood in science and technology studies.

[19] This has been stated unequivocally by the European Court of Human Rights – to which Russia is subject, as a member of the Council of Europe – that, in four different judgments delivered in June 2020, criticized the Russian law for allowing the government to take down or block online content without requiring a court order. An interesting analysis of the four judgments (*Flavus and Others* v. *Russia*, *Bulgakov* v. *Russia*, *Engels* v. *Russia*, and *Vladimir Kharitonov* v. *Russia*) is offered by G. Grover and A. Thomas (2021).

[20] See the dedicated section on the website of the Bank of Russia www.cbr.ru/eng/psystem/. Mir literally means "peace" or "world" in Russian. Interestingly, the Mir payment system has the same name of the space station, operated from 1986 to 2001 by the Soviet Union and later by Russia.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

payment system established in 2014 to overcome total denial of e-payment service imposed on Russian banks by US-based Visa and MasterCard. After the annexation of Crimea, US sanctions against Russia left millions of Russian customers with no access to credit card services. As a response, the Central Bank of Russia established Mir that is fully operated by the Russian National Card Payment System, a subsidiary of the Central Bank of Russia. This episode demonstrated that digital sovereignty initiatives often emerge out of the perceived risks of disruption and the possible weaponization of foreign technologies on which a country, an individual, a community, or a corporation relies.

Similar considerations can be seen in the ambitious plan of BRICS countries, chiefly China and Russia, to develop their own national digital currencies[21] in a bid to compete with and reduce dependence on the US dollar at the international level, enabling a process of "dedollarization" (Huang, 2020). Furthermore, as stressed by Hariharan and Natarajan in this volume, the consequences of the Visa-MasterCard episode are far from trivial and represented a further wake-up call for the BRICS nations, only one year after the NSA scandal. Increasingly aware of the risks linked to overreliance on foreign technology, India launched the development of its indigenous payments system, the Unified Payments Interface (UPI) and the National Payments Corporation of India (NPCI), as well as the Digital India[22] program. As we will argue in the following section, the ultimate goal of the latter plan is the development of a digital public infrastructure (DPI) that enables India's digital transformation by fostering the emergence of a sound national digital ecosystem and reducing the country's reliance on foreign hardware and software, thus reasserting digital sovereignty.

Lastly, it is also interesting to note that similar concerns and increasing alignment of Russia and India regarding the relevance of their digital sovereignty on electronic payment systems also emerged from the countries' explicit political statements. Indeed, in late 2021, India and Russia expressed interest in enhancing their cooperation toward the mutual acceptance of national payment systems within their respective national payment infrastructures, promoting "interaction of Unified Payments Interface (UPI) and the Faster Payments System of the Bank of Russia (FPS). [In this occasion, t]he Russian Side invited Indian credit institutions to connect to the financial messaging system of the Bank of Russia to facilitate faultless interbank transactions" (Ministry of External Affairs of India, 2021).

Importantly, the relevance of digital payments systems is fundamental from a state digital sovereignty perspective, especially for giant countries with large populations such as the BRICS. On the one hand, e-payments have been traditionally controlled by dominant US providers such as Visa and MasterCard,

[21] A detailed analysis of the ongoing BRICS initiatives in this context can be found consulting the recording of the "BRICS Conference – Central Bank Digital Currencies" (CyberBRICS, 2022).

[22] Digital India was launched in 2015. See www.digitalindia.gov.in.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

thus creating an enormous vulnerability for all countries relying on such systems, as the abovementioned Russian example illustrates tellingly. On the other hand, electronic payments have garnered major relevance due to the enormous amount of data and revenue they generate. Aware of the strategic importance of e-payments, BRICS nations have heavily invested in this data-intensive sector.

In less than a decade, China, India, and Brazil have become global leaders in instant online payments, leapfrogging virtually all developed countries (ACI Worldwide & Global Data, 2022).[23] India and China have achieved the first and second positions of the global ranking of countries with highest number of real-time online payments. Even more impressively, Brazil has reached the top ten of the ranking, starting from the bottom, in only two years since the introduction in 2020 of Pix, its national digital payment system established by the Brazilian Central Bank.[24] Although not always mentioned explicitly, digital sovereignty is becoming the key concern underpinning new digital payment initiatives in the BRICS. Pix is now used by 70% of Brazilians to transfer money at no cost, while before its introduction the only available option to process instantaneous electronic payments was to use the networks of foreign e-payment giants such as Visa and MasterCard, which charge a 3% fee on each transaction besides centralizing data collection of all their users (Belli, 2023). These latter points are the main reasons why the development of public digital infrastructures such as Pix are enormously relevant from a "good digital sovereignty" perspective: it democratizes digital payments, reduces market and data concentration, and provides unique insight onto the national economy to the Central Bank of Brazil (rather than to two foreign actors), thus reverting a trend many scholars have defined as data colonialism (Belli, 2023).

This concern was evident in the Brazilian Central Bank's order to suspend the plan of WhatsApp – the dominant instant messaging app in Brazil, owned by the US conglomerate Meta – to introduce the app's own payment system several months before the release of the Pix payment system (Mandl & Versiani, 2020). The rationale of the Brazilian Central Bank's order is that the first mover advantage of WhatsApp – the use of which is subsidized to consumers by all Brazilian operators in the context of the so-called "zero-rating" schemes[25] – would have created "irreparable damages" to competition,

[23] Particularly interesting and up-to-date data are available in the ACI Worldwide and Global Data reports on "Prime-Time for Real Time," which track and analyze real-time payments volumes, growth, and dynamics of 48 global markets.

[24] According to the ACI Worldwide and Global Data report mentioned at n.42, "Brazil's Pix system has gotten off to a flying start, passing a billion transactions within months of launching and continuing to go from strength to strength. There are now more than 100 million Pix users" (ACI Worldwide & Global Data, 2022, p. 8).

[25] For a detailed analyses of zero-rating practices, see www.zerorating.info. For an updated overview of the practices in Brazil, see Instituto Brasileiro de Defesa do Consumidor [IDEC] and Instituto Locomotiva (2021).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

privacy, and data protection in Brazil. Hence, the suspension of WhatsApp's plan was necessary to "preserve an adequate competitive environment that can ensure the functioning of a payment system that is interoperable, fast, secure, transparent, open, and cheap" (Banco Central do Brasil, 2020).

We are witnessing a new generation of techno-regulatory initiatives that aim at embedding digital sovereignty into technology. This new approach to policy and regulation by technology, seen from the BRICS experiences, deserves academic, policy, and public attention. While not necessarily a trend toward techno-authoritarianism where technology becomes an instrument of control, embedding digital sovereignty into technology can also be a positive exercise of self-determination. The India Stack, for instance, fosters the digitalization of the entire country through the development of digital public goods based on open source technology. It is a fascinating example of digital sovereignty fostered by the state but implemented in a decentralized way by technologists through technology, no less effective than state policy. This and other initiatives from BRICS and the Global South need to be carefully studied and understood by researchers, policymakers, and civil society advocates alike, as it holds promise to a future shape of governance, policy, and regulation.

10.4 Resistance to Data Colonialism or Construction of Digital Protectionism?

Digitalization can enable important benefits but depending on how such a process is structured, it may also entail considerable risks for state digital sovereignty. Such considerations particularly relate to extensive adoption of foreign software, introducing risks spanning from unsustainable dependence of both private and public sectors on foreign technology to various threats to national security, uncontrolled extraction of strategic national resources – notably (personal) data of entire populations and economic sectors – and unfair competition. In this perspective, as we have noted in the introduction, Brazil was a pioneer of software autonomy through a Commons Digital Sovereignty stance more than two decades ago.

Indeed, the Lula administrations of the 2000s realized that by being a mere software consumer, Brazil was facing an unsustainable future, destined to be a digital vassal like most other countries. In retrospect, the Free Software policies adopted by Brazil 20 years ago – and unwisely reversed, under the Temer administration – were remarkably forward-looking in reducing software dependency and public expenditure, while enhancing security and control over Brazilian digital infrastructures. Even if these policies have never been explicitly labeled as "digital sovereignty," they are some of the earliest and strongest examples of State Digital Sovereignty.

It is also necessary to stress that digital sovereignty policies may also be primarily driven by economic protectionism. Indeed, a further element of

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

complexity in digital sovereignty discussions is the potential protectionist dimension. Digital sovereignty narratives lend themselves well to the inclusion – and to some extent confusion – of a variety of goals, including resistance to data colonialism (Ávila, 2018), the implementation of digital development agendas, the establishment of protectionist measures, the tightening of social control, and political exploitation of post-colonial resentments.

Digitalization can enable important benefits but, depending on how such a process is structured, it may also entail large risks. China and India provide interesting insight in this regard. While the Snowden revelations have triggered vitriolic reactions in the Brazilian government and boosted Russian plans for "internet sovereignty," the Chinese authorities perceived them as exposing China's vulnerable position as long as it relied on foreign technology. The Chinese approach to digital technology has been extremely cautious, understanding not only the potential of digital technologies to foster development but also the importance to assert control at the national level.

From the perspective of the Chinese authorities, the 2013 Snowden revelations and the 2014 US sanctions on Russia have exposed both external and internal threats. The reliance on and limited control of foreign technologies undoubtedly created vulnerabilities for both external and internal actors. Furthermore, China perceived its strategic disadvantage in a global digital economy dominated by US technologies, as well as a situation of weakness in a global digital governance landscape dominated by Western actors' narratives. Clearly, in the Chinese authorities' view (Arsène, 2016), this situation called for an immediate and organized reaction, carefully blending policies, politics, and developmental approach to redefine Chinese digital sovereignty.

In 2014, the Xi Jinping administration established the Cyberspace Administration of China (CAC) and the Central Commission for Cybersecurity and Informatization, creating a new cybersecurity and informatization *xitong*, a cluster of institutions with various digital-related competences, which has been personally chaired by Xi Jinping to date (Creemers, 2020). In the same year, the first World Internet Conference (WIC) was organized, creating a China-led global multi-stakeholder forum on digital governance. The first *Wuzhen Declaration*, proposed as a WIC outcome, featured "cyber sovereignty" in a prominent position among the advocated principles. In the following year, at the opening ceremony of the WIC 2015, President Xi Jinping himself stressed the importance of every country's right "to choose its online development path, its network management model and its public Internet policies, and to equal participation in international cyberspace governance" (Xi, 2015).

Simultaneously, China started paying more close attention to digital innovations. It is hoped through innovations Chinese researchers, developers, and ultimately the Chinese state could achieve a sovereign position rather than relying on existing Western, mainly US, technologies. Due to reduced production costs and increasing advancement in Chinese technology competitiveness,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

the production and large-scale exportation of Chinese hardware seemed to have solidified and expanded the Chinese state's digital sovereignty. Not surprisingly, the Internet of Things (IoT), featured as a prominent area of the "Made in China 2025" strategic plan in 2015, aimed to expand China's development of connected devices to reach 95% of the market by 2025. Such ambitious goals were part of the comprehensive "Digital Silk Road" initiative and the larger Belt and Road Initiative (Jiang, 2021).

Artificial Intelligence (AI) appears to be another area of essential importance for the preservation and expansion of Chinese digital sovereignty. The Chinese State Council issued an *AI Development Plan* in July 2017, prompting various initiatives from local governments and businesses to establish AI funds and local plans with the goal of becoming the world's "primary" AI innovation center by 2030 (Ding, 2018). The goal of such a plan aims to reproduce the success of the State Council 2015 Plan for "mass entrepreneurship and mass innovation" that created thousands of technology incubators, entrepreneurship zones, and government-backed funds in attracting an enormous level of private venture capital.[26] At the same time, since 2018 China has started piloting the inclusion of computer coding in the curricula for primary and middle school students. Since 2020, such curricula were incorporated into national planning, denoting a clear understanding of the key role of digital capacity building to achieve full digital sovereignty (Zou, 2020): only a country whose population knows how to develop and use digital technologies can truly be digitally sovereign.

Hence, apart from the yearning to resist US intelligence programs, BRICS countries initiatives demonstrate that an equally, if not more, relevant preoccupation is the preservation and expansion of the local digital economy while avoiding digital colonization. However, understanding, planning, coherence, and implementation capabilities of each BRICS country vary enormously, spanning from a holistic Chinese approach to more fragmented or even unorganized postures.

BRICS policies and initiatives also vary in their understanding of the structural power of technology. As mentioned in the introduction of this chapter, awareness of the structural power technology plays is essential to understand the relevance of digital sovereignty and, chiefly, how to organize the concrete implementation of this multifaceted notion. However, not all BRICS countries and the individuals, the entities, and communities that compose them may have achieved the same understanding of this issue. Due to their reduced size and power (whether a BRICS member or not), they may not even be able to elaborate any measure to resist digital colonization, even if they wished to do so.

[26] The State Council directives were issued as a response to Prime Minister Li Keqiang call for "mass entrepreneurship and mass innovation" on September 10, 2014, during the 2014 edition of the World Economic Forum's "Summer Davos" in the coastal Chinese city of Tianjin (Lee, 2018, p. 70).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

In this context, Vashishta Doshi and Henrique Delgado's contribution to this volume reminds us that US technology providers are at the core of the digital economy. It is through the likes of tech giants such as the notorious GAFAM (Google, Amazon, Facebook, Apple, and Microsoft) and more recently OpenAI and Nvidia that the US maintains an upper hand in the technology field, exercises its digital sovereignty, and expands this power globally. Reliant on US digital infrastructures, middle powers such as Brazil and India as well as most other countries find themselves in a situation of at least partial digital colonization, where the only available option to undertake a "digital transformation" is the use of foreign digital products and services.

In this perspective, the Digital India initiative focuses on the three digital architecture layers that are considered essential enablers of digital sovereignty: expansion of connectivity, digitization of public services, and establishment of DPI. The Indian government is aware of not only the key role of digital connectivity but also the fact that not all types of internet access offerings are equal and existing differences may have enormous impact on national and community digital sovereignty. It is interesting to note that one of the most assertive and impactful digital sovereignty measures established by India over the past decade has been the adoption of strict Net Neutrality regulation in 2016, prohibiting the so-called "zero-rating"[27] practices where a few dominant US platforms such as Facebook offered "free" access to the unconnected population as a purported inclusive access initiative (Belli, 2017a).

While these plans were heralded as a way to "connect the unconnected" by their proponents, the opponents to such practices have stressed that sponsoring access to a few dominant apps would have exacerbated the dominance by a few foreign commercial actors. Simultaneously these practices can considerably increase data concentration in the hands of the few sponsored platforms, creating strong dependence on such services in the entire (developing) world (Belli, 2017a). To understand the zero-rating services especially in low- and middle-income countries where average individuals cannot afford internet access fees, it must be considered that for the largest application providers, it is worth sponsoring internet access limited to their applications to enlarge and retain user base to perpetuate user dependency on such applications.[28]

We may fairly assume that when the Indian government decided to prohibit the zero-rating practices, one of the main goals was not only to preserve internet openness, competition, and free expression, but a key consideration behind India's decision to prohibit zero-rating services was mainly to avoid the concentration of Indian internet users and the consequent collection of Indian user data in a few foreign apps, capable to exert enormous control, extract

[27] For an analysis of zero-rating practices, see www.zerorating.info.

[28] The importance for businesses to "hook" users into their applications, through an ample range of techniques including also addictive interface configurations, is eloquently presented by N. Eyal (2014).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

enormously valuable insights and profits under foreign tax law, store user data in foreign servers, enhance foreign software and AI development thanks to such data, and sharing them with foreign intelligence agencies through numerous programs revealed by the Snowden episode.

Hence, the 2016 order of the Telecommunications Regulation Authority of India (TRAI) prohibiting zero-rating practices denotes the same "digital sovereignty" rationale applied by the Brazilian Central Bank to the suspension of WhatsApp Payments to preserve openness, competition, and data privacy in the Brazilian digital payment system. Indeed, BRICS institutions seem to have an increasingly sophisticated understanding of the digital colonization dynamics underpinning the provision of "free services" by dominant foreign tech giants, notably regarding the fact that such services, presented as free, are de facto paid with a waiver on the individuals' and country's possibility or ability to exercise sovereignty over data (Belli, 2021b).

Clearly, the use of foreign technology is not something negative per se as long as such technology does not become a Trojan horse aimed at undermining capability of the user – be this an individual, a corporation, a specific community, or a country – to exercise (digital) self-determination. In this spirit, the considerable increase in digital policies and notably data-related regulations in the BRICS in recent years may be seen as a clear reassertion of digital sovereignty to protect critical national resources. It is useful to recall that together Brazil, Russia, India, China, and South Africa are home to 3.2 billion people, representing roughly 42% of the world's population. In effect, BRICS countries sit on 42% of "the most valuable resource" (The Economist, 2017) on the planet: personal data (Belli, 2021a, 2021b).

Members of the BRICS grouping are aware not only that they are the main producers of personal data but also that higher levels of connectivity concretely would produce more wealth and productivity.[29] They have also developed an increasing understanding that digital services provided by foreign corporations and portrayed as "free" are not exactly so, but rather paid with an open-ended license to extract personal data and, ultimately, undermine state and individual digital sovereignty. This situation has become even more palpable in the context of the ongoing "scramble for data," launched by dominant tech businesses. This rush to offer "free" digital services to developing countries may indeed be seen as a strategy to be the first in capturing the attention of poor users and drilling as much data as possible out of

[29] According to the World Bank, 10% increase in broadband penetration can result in a gross domestic product growth of up to 3.2%, with benefits ranging from the generation of services and jobs to an increase in family income (World Bank, 2016). The Organization for Economic Cooperation and Development and the Inter-American Development Bank have underscored that the expansion of connectivity generates greater availability and efficient use of services, enhancing social inclusion, increasing productivity, and improving governance (Organization for Economic Cooperation Development and Inter-American Development Bank, 2017).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

entire populations who frequently lack data protection frameworks to prevent undue exploitations. The indigenous populations are increasingly seen by the new digital colonizers as convenient data wells.

As argued in this book, digital infrastructures play a particularly relevant role to structure digital sovereignty. Hence, it is obvious that India's Net Neutrality regulation, its ban of zero-rating services, together with the Digital India program have been essential to reducing India's exposure to foreign digital sovereignty and building its own. The simultaneous promotion of connectivity and ban of zero-rating practices paved the way to the entrance of Reliance Jio, a new domestic player, in India's mobile internet market, which with its low-rate offering managed to reduce gigabit prices by almost 95%, double the number of connected Indians and increase more than twentyfold data consumption in less than 5 years.[30] To capitalize on such a staggering expansion of connectivity infrastructure, Digital India fostered the creation of a set of Application Programming Interface (APIs)[31] commonly referred to as the "India Stack"[32] that play a key role in India's DPI, on top of which new home-grown digital services can be built.

10.5 DISORDERED APPROACHES TO DIGITAL SOVEREIGNTY

BRICS countries have developed an understanding of the strategic importance of data, software, and infrastructures to constructing digital sovereignty. Data is an essential resource used as raw material to develop AI applications by powering highly complex algorithms. Software, on the other hand, plays an essential role in creating "high-growth, high-margin, highly defensible businesses" (Andreessen, 2011) as an increasingly large number of industries are redefined by software. From the automation of agriculture and manufacturing to the digitization of public services and personal apps in our smartphones. "Software is eating the world" famously stated by Marc Andreesen. The stellar market evaluation of some technology giants means that in practical terms if a digital sovereign – be it a corporation or a nation-state – can exercise control over popular software, it may earn very large returns on investments. Conversely, one is likely to perpetually pay a usage fee along with the contractual conditions unilaterally defined by the digital sovereign over digital infrastructure, data, services, and protocols.

This latter point is of utmost importance, especially when industry segments are increasingly automated by large-scale usage of software (or AI). When the software in question is not owned by the user, it is highly likely that in the long

[30] Compare the Indian Telecom Services Performance Indicator Report developed by the Telecom Regulatory Authority of India www.trai.gov.in/release-publication/reports/performance-indicators-reports.

[31] An API is a piece of software that allows different software applications to interact and exchange data, according to the specifications established by the API.

[32] See www.indiastack.org/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

term, the main beneficiary of such automations will be the software producer, that is, the digital sovereign. Admittedly software automation will generate efficiency gains for users and price will likely decrease, and some services may even be provided "for free." However, when such services are not paid with money by users, they are paid with user data. This shift in payment either through a fee to the software provider or through personal data or both is the de facto payment with the user's individual sovereignty, which entails a choice between self-determination and dependency.

It is understandable that different digital sovereigns, as with their different capacity to muster, develop and deploy digital infrastructure, data, service, and protocols, follow their own agendas and interests, which frequently conflict with those of others. Several BRICS countries, notably Russia, India, and China (RIC), have developed an increasingly systemic thinking about digital sovereignty that can lead to positive or negative outcomes. Brazil and South Africa, on the other hand, may have had intended to do so but have struggled to develop or implement a coherent vision, due to unstable political environments, inconsistent policies, or timid implementation of such policies.

Brazil offers, again, a telling tale. While it reacted vehemently when attempts in undermining its digital sovereignty were revealed, its posture denotes a certain disorder, typical of most politically unstable countries aspiring to achieve digital self-determination and independence from foreign technology. The fact is that shortly after condemning NSA surveillance, former President Dilma Rousseff actively promoted the zero-rating service offered by Facebook in Brazil (Belli, 2015), thus opening the path for the digital colonization of the country[33] by a foreign corporation. That Facebook to date has been cooperating with US intelligence agencies such as the NSA suggests President Rousseff's promotion of free-rating services can be now seen as a willful waiver of Brazil's state digital sovereignty.

It is interesting to note that, according to recent research by the Brazilian Institute for Consumer Protection (IDEC), 85% of Brazilian mobile users have prepaid plans including limited data volumes and zero-rated social networks (typically WhatsApp and Facebook) (IDEC & Instituto Locomotiva, 2021). Due to the subsidized nature of such apps, this enormous part of the Brazilian population utilizes the internet primarily to access US-based social media, especially in the last part of a month when the data allowance is entirely consumed and the only accessible applications are the zero-rated ones, which become also the only ones with concentrated data collection. It is difficult to think that the Brazilian government does not realize that this

[33] It is important to stress that, despite multiple years of permissive attitude of Brazilian regulators toward zero-rating, this practice amounts to preferential treatment of applications, which is prohibited under Brazilian net neutrality norms, such as art 9 of the Internet Civil Framework and art 9 of Decree 8771/2016.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

situation implies the cession to foreign actors the right to extract personal data from the entire connected population and generate enormous and nearly untaxed profit with value generation on foreign servers.

Another remarkable example illustrates the confused and even conflicting Brazilian approach to digital sovereignty. In the context of its privatization program, the Bolsonaro administration announced in 2019 the intention to sell two public enterprises deemed the crown jewels of Brazilian IT: the Federal Data Processing Service or *Serviço Federal de Processamento de Dados* (Serpro) and the Information Technology for Pensions Corporation or *Empresa de Tecnologia e Informações da Previdência* (Dataprev). Serpro is the largest government-owned corporation of IT services in Brazil, created in 1964 to modernize strategic public sector. Dataprev is a Brazilian public company, responsible for managing the Brazilian Social Database with five software development units and three data centers throughout the country. Both are under the control of the Ministry of the Economy.

These corporations including the software they produce and the enormous databases they control are highly valuable strategic assets in terms of digital sovereignty. While selling these corporations to foreign investors could generate considerable financial gains, it would also incur many unintended consequences for Brazil's state digital sovereignty. After several years of feasibility studies, the Brazilian Congress has kept postponing selling these state assets until it reached the electoral period when the sale of state-owned enterprises becomes de facto impossible (Lobo, 2022). The strategy of the Brazilian Congressmen has been effective, even unorthodox, to achieve the preservation of the two public companies and their digital assets. However, the episode goes far beyond highlighting the lack of understanding of the implications of digital sovereignty of the Bolsonaro administration. It explains tellingly the dependency of digital sovereignty on politics and public policies.

Such dependency became clear with the recent change at the helm of the Brazilian federal government. One of the first executive orders adopted by the new Lula administration has suspended the privatization of public companies deemed as nationally strategic assets, including Serpro and Dataprev (Presidência da República, 2023). While such reversal indicates a welcomed renewed sensitivity to digital sovereignty issues, it also proves that in most countries as in Brazil digital sovereignty policies are ultimately a function of politics.

Corporate digital sovereigns – typically large business actors – build and manage expansive digital infrastructures with their own agendas to fostering self-interest that may conflict with the interest of other sovereign entities using the technology they supply, which could include their users, advertisers, and the public they purportedly serve. Further, private developers of digital infrastructures may become proxies for the expansion of State Digital Sovereignty where they are headquartered. As demonstrated by the Snowden revelations and as contended by Stefano Calzati in his contribution for this

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

book, the expansion of digital infrastructures and services overseas makes it possible for a given state to project its digital sovereignty well beyond its borders, whether American or Chinese.

It is also essential to note that initiatives branded as digital sovereignty may be frequently used to disguise ambitions to intensify control through digital means. The reader might think of China and Russia as frequently suggested examples in this sense, but such ambitions are rather widespread well beyond these two countries. As stressed by Enrico Calandro's contribution to this volume, South African digital sovereignty discourse finds itself at the crossroad of securitization and ICT development, as happens in many other African countries.

South African authorities as well as other developing countries have a considerable opportunity to construct solid basis for digital sovereignty through more modernized digital policies to properly regulate the functions and consequences of ICTs. For South Africa, the state construction of digital sovereignty aims to enhance self-determination, cybersecurity, and the rule of law in the digital environment. At the national level, South Africa has also stressed "data ownership, data sovereignty, and data protection are critical elements for the digital economy" (Department of Communications & Digital Technologies, 2021, p. 20). In April 2021, the South African government presented its Draft National Data and Cloud Policy Data, which explicitly recognizes that and "seeks to strengthen the capacity of the State to deliver services to its citizens, ensure informed policy development based on data analytics, as well as promote South Africa's data sovereignty and the security thereof" (Department of Communications & Digital Technologies, 2021, p. 8).

As for any government, however, it is also very tempting to utilize the digital sovereignty narrative to expand state control over computer systems and digital communications, facilitating surveillance and online censorship. For instance, in October 2019, South Africa adopted the Films and Publications Amendment Act (2019), dubbed "Internet Censorship Law" (Vermeulen, 2022), which allows the South African content regulation authority, the Film and Publication Board, to request the removal of any content deemed harmful. It went into effect in 2022. According to the law, any internet service provider (ISP) with knowledge that its service is being used to distribute or host content that incites imminent violence, serves as propaganda for war, advocates hatred against a person or an identifiable group, or sexually exploits children must immediately remove the content and communicate the identity of the person who published the prohibited content to the Film and Publications Board or the South African Police Services.

South Africa offers an interesting example. On the one hand, the country has recently enacted and adopted progressive data protection and cybersecurity legislations. On the other hand, it has simultaneously established a securitization agenda and increasing censorship measures in reaction of cyber threats (Belli, 2021c). Similarly, while South Africa is home to several

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

outstanding examples of Commons Digital Sovereignty, spanning from community networks to smart villages, led by empowered local communities, it also simultaneously advocates a number of "Fourth Industrial Revolution" policies opening the path to a large number of data colonialism practices (Benyera, 2021).

10.6 CONCLUSION: DIGITAL SOVEREIGNTY OPTIONS

An agnostic approach to digital sovereignty in the BRICS acknowledges that different digital sovereigns may pursue self-determination, cybersecurity, and control with different goals and outcomes. These leave us fundamentally with three options to structure digital sovereignty. The first one is a form of hard digital sovereignty amounting to near digital isolation of the digital sovereign in order to exercise the highest possible level of control and the establishment of tightly controlled gateways to regulate information exchanges. This option might be the most effective choice for isolated communities willing to create their own intranets to communicate among themselves without necessarily communicate with the rest of the world – as even some community networks do (Belli, 2017; GISWatch, 2018) – or countries eager to build strong control on their national segment of the internet and tightly regulate communications, such as China and Russia, but it can only be afforded in the long-term by those that can manage to be digitally self-sufficient and thrive, even while being relatively isolated.

The second option, which is ideal in the opinion of these authors, would be shared global rules to frame and regulate digital technologies and their uses, providing a leveled regulatory playing field, so that any entity would have an incentive to cooperate rather than engaging into antagonist behaviors. Unfortunately, while this option would be ideal, it seems highly unlikely it could be easily reached, given the considerable conflicting interests at stake, the lethargic times of international policymaking, the considerable intellectual and financial resources needed to implement this option in practice, and the democratic deficit of which many intergovernmental organizations – on which such option would have to rely – are frequently accused.

The third and final option seems also possible and palatable. It consists of the establishment of regional blocks or aligned groupings that share common – or at least (legally) interoperable (Belli & Doneda, 2022; Belli & Zingales, 2023) – regulatory frameworks and technological tools. Such groups may limit information flows and technology exchanges with other blocs to the few sectors where shared agreements exist. This option would be less ideal than the establishment of shared global norms and technologies, but would have the benefit of facilitating international exchange, attracting entities with less restrictive digital sovereignty thinking toward other areas, thus increasingly enlarging overlapping areas of interest. As such, different areas would also compete, attracting an ever-larger number of entities and expanding their system globally.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

This latter option seems particularly interesting for BRICS countries in light of the grouping's recent expansion (BRICS, 2023) as well as their commitment to enhance cooperation on digital policy frameworks with particular regard to cybersecurity issues. At the 15th BRICS Summit, chaired by South Africa in August 2023, the grouping's heads of states "have decided to invite the Argentine Republic, the Arab Republic of Egypt, the Federal Democratic Republic of Ethiopia, the Islamic Republic of Iran, the Kingdom of Saudi Arabia and the United Arab Emirates to become full members of BRICS from January 1, 2024" (BRICS, 2023). It is clear that the inclusion of these new partners in the grouping hopes to expand the BRICS role as a gathering hub of Global South regional leaders, especially by strengthening the presence in Africa (e.g., Ethiopia hosts the headquarter of the African Union) and including some the most influential countries from the Middle East region, which have already acquired significant global relevance. Such a move becomes particularly relevant in the context of the Ukraine and Gaza wars, which have created enormous instability and prompted many countries to reassess and redefine their strategic alliances and their value chains, desperately looking for strategic autonomy and stability.

Such a scenario has obvious ramifications in digital affairs. In this context of the recent cybersecurity, commitments of the BRICS leaders sound prescient. Indeed, since the New Delhi Declaration, issued as an outcome of the 2021 BRICS Summit, the bloc's leaders expressed the intention to:

> [...] advance practical intra-BRICS cooperation in this domain, including through the implementation of the BRICS Roadmap of Practical Cooperation on ensuring Security in the Use of ICTs and the activities of the BRICS Working Group on Security in the use of ICTs, and underscore[d] also the importance of establishing legal frameworks of cooperation among BRICS States on this matter and acknowledge[d] the work towards consideration and elaboration of proposals, including on a BRICS intergovernmental agreement on cooperation on ensuring security in the use of ICTs and on bilateral agreements among BRICS countries (BRICS, 2021).

The elaboration of such legal frameworks and intergovernmental agreement would be a useful test bed to gauge the extent to which such cooperation can exist in practice. Cybersecurity issues, and notably cybercrime, as well as most digital policies that would fit into the large state digital sovereignty umbrella, are intimately intertwined with strong economic and political interests of each digital sovereign and grounded on quintessentially domestic cultural and legal particularities. The attractiveness of the BRICS bloc remains unchanged, even if some of the countries might have underperformed the original predictions that led to the creation of this bloc. Such attractiveness would notably increase, should BRICS countries create a BRICS digital sovereignty area with shared and compatible digital policies.

A scenario where the BRICS promote legal interoperability would allow the grouping to act as a platform to conjugate digital sovereignty with openness

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014

and inclusion (Belli & Doneda, 2022; Belli & Zingales, 2023). This could be an even more powerful strategy considering the current context of expansion of the BRICS through the BRICS+ initiative (Razumovsky, 2022). On the one hand, this scenario would allow the BRICS to fulfill its fundamental mission of fostering international cooperation and building a multipolar order and inclusive global governance, led by the Global South for the benefit of developing countries. On the other hand, this would also allow the BRICS to act both as an "integrator of integrators," fostering the interoperability of regional projects where the participating countries are leaders (Eurasian Economic Union, Mercosur, and South African Customs Union) and as a "union of regionalisms," where regional associations (African Union, Community of Latin American and Caribbean States, and SCO) can interoperate thanks to compatible normative frameworks (Razumovsky, 2022). Sovereignty and openness can and should be seen as mutually reinforcing rather than as antithetic goals that can and should be pursued simultaneously. BRICS have the potential to demonstrate that the Global South can lead in digital governance, promoting openness while preserving sovereignty: as former Brazilian President Luiz Inacio Lula da Silva – generally known as Lula – noted, "the logic behind BRICS [is] to do something different and not copy anybody […] trying not to be dependent" (Escobar, 2019; Prashad 2012).[34]

[34] It is useful to remember that many Global South countries have been denied the full enjoyment of human rights, democracy, and rule of law by Western colonizers and suffered remarkably abusive treatments for many decades or even centuries. Often, these countries gained independence only after incredibly violent wars that in some cases lasted many years and ended less than fifty years ago. For a brief but detailed description of the geopolitical changes from 1900 to 2000, see The National Archives (n. d.).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 21:37:04, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009531085.014