Pre-print version of Luca Belli & Min Jiang. Digital Sovereignty from the BRICS: Structuring Self-determination, Cybersecurity, and Control. in Jiang M. & Belli L. (Eds) Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press. (2024)

Digital Sovereignty in the BRICS Countries

Luca Belli and Min Jiang, *Co-Editors*

Conclusion

Digital Sovereignty from the BRICS:

Structuring Self-determination, Cybersecurity, and Control

Luca Belli[1]

Min Jiang[2]

FGV Law School[1]

University of North Carolina – Charlotte[2]

Abstract

This chapter acknowledges both the fluidity and the complexity of the concept of digital sovereignty, while also highlighting the necessity to consider digital sovereignty strategies, policies, and governance mechanisms from a holistic and long-term perspective. The chapter notes that digital sovereignty plays a pivotal role in fostering self-determination, while increasing cybersecurity and strengthening the control capabilities of the "digital sovereign". Importantly, depending on the policy or initiative at stake, the "sovereign" can be an individual, a community, a corporation, a state, or a group of states. Here, we take an agnostic approach to digital sovereignty, exploring a selection of practices and providing insight into what this concept means in practical terms. Indeed, digital technologies can facilitate enormous advancements to be put at the service of people, but can also be weaponised against individuals, corporations, and nation states. BRICS countries' approaches offer some telling examples of not only how and why the need for digital sovereignty can emerge, but also how dysfunctional the implementation of digital sovereignty policies may become without a coherent and long-term vision. Ultimately BRICS experiences illustrate that enhancing a digital sovereign's self-determination, cybersecurity, and control is likely to reduce the undue influence of other digital actors. However, the success of a digital sovereignty strategy largely depends on the understanding, consistency, resourcefulness and, ultimately, organisational capabilities of aspiring digital sovereigns.

Introduction: Digital Sovereigns or Digital Subjects?

This chapter acknowledges both the fluidity and the 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 first chapter of this volume, 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 conceptualisations of this notion as well as its concrete implementations in BRICS countries allows us to move beyond the conventional, normative, state-centric approach towards "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 control of the various types of "digital sovereigns". Importantly, depending on the conception of digital sovereignty that we decide to utilise and the initiatives at stake, a "digital sovereign" can be an individual, a community, a corporation, a state, or even a supranational organisation[2].

Indeed, the examples analysed in this volume illustrate how individuals, communities, corporations, states, and supranational organisations can become digital sovereigns by

---

[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, i.e. the right to freely determine and pursue one's economic, social and cultural development, 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

[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).

understanding, developing, and mustering the use of digital technologies. On the contrary, 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 as something positive or negative, depending on who is the sovereign entity is. 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 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 and control. In this perspective, a digital sovereign is the entity that owns, operates and, ultimately, exerts control on how technology can and will be used. To understand the breath and relevance of digital sovereignty it is therefore useful to emphasise 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,

[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, the International Covenant on Civil and Political Rights.

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 between people, organisations, businesses, and states. The sovereign defines where walls or doors will be in the labyrinth, thus ultimately exercising power by controlling 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 behaviours 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 realising 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 as digital sovereigns as they are not only regulated by technologies but also enjoy self-determination thanks to technology and

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

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 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 development (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 byproduct of communities yearning for network self-determination (Belli & Hadzic, 2021). Indeed, such examples demonstrate that even vulnerable and marginalised communities such as Brazilian *quilomobola*[6] women or rural communities and slum-dwellers in South Africa

[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, i.e., to "pursue their economic, social and cultural development" through the opportunities that connectivity can offer. (Belli, 2017b)

[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 colonisers in the 16th century and maintained until 1888. The inhabitants of these communities are called quilombolas. With the

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.

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 colonised) 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 weaponised against individuals, corporations, and nation states. In such contexts, this chapter takes a more agnostic approach towards 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.

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.

---

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)

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 U.S., 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 towards the U.S. but have also associated dependence on US technology with high risks.

A telling example is the existence of alternatives to the Global Positioning Systems (GPS), the latter established by the U.S. in the late 70s. GPS, an essential component of a wide range of digital products and services, plays a critical role for many for military technologies used for defence purposes. Out of the five alternatives to the dominant U.S. 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 colonisers, feeding several decades-long engagements in "South-South cooperation" (The South Commission, 1990)[10] – through numerous initiatives,

---

[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 Organisation (SCO), a larger alignment that also includes China and Russia.

[8] The Global Navigation Satellite System (GLONASS) was developed by Russia in the 80s; 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, emphasising 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 organisation established in 1995. https://www.southcentre.int/

such as the Group of 77, the Non-Aligned Movement and Group of 15, the IBSA Trilateral[11] and, finally, the BRICS grouping[12] – to strong sensitivities due to the U.S. 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 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 reorganising their postures to enhance their cooperation on digital matters – especially in cybersecurity (Belli, 2021a; Belli, 2021b; Belli, 2021c) – as a reaction to the unlimited digital sovereignty exercised by the U.S. 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

---

[11] Little known to the public, IBSA is a trilateral forum which 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 http://www.ibsa-trilateral.org/ This organisation become well-known to Internet 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 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. See Judgment of 15 December 1983, BVerfGE 65, 1-71, Volkszählung 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. (The Brazilian General Data Protection Law – Unofficial English version, 2020).

the “weaponization” of digital policies was the Trump Administration which 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 U.S. 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 self-determination.[14] While such concerns have been particularly acutely felt amongst 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 conceptualisation for recognising 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 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 by Western observers, to a mainstream issue now advocated by EU leaders as an essential tussle to reassert strategic autonomy.

Resisting Foreign Espionage, Meddling and Sanctions

We must note that the various initiatives that emerged over the past decade in 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 U.S.’s

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

invasive behaviours through its technological apparatus has led BRICS countries to realise that without alternatives, their technological disadvantage would have led to irreversible economic dependence and ultimately (digital) colonisation.

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 notorious Schrems II case invalidated the Trans-Atlantic transfer of personal data from the EU to the U.S. due to the nature of U.S. 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 towards dominant U.S. technologies, it is instructive to consider the normative analysis of the ECJ. Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorises the collection, use, and dissemination of electronic communications content stored by U.S. platforms (such as Facebook, Google, Microsoft, etc.) or transported across the Internet's "backbone" infrastructure, thus compelling US connectivity providers (such as AT&T, Verizon, etc.) 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 Roussef's opening remarks at 68th UN General Assembly, describing the NSA scandal in the following terms:

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

> "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) As a consequence, 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 fibre optic cable. This cable connects Seixas, Portugal directly with Fortaleza, Brazil without having to pass through Miami, U.S., where all previous submarine cable landed as part of U.S. telecom backbone. The inauguration of Ellalink in June 2021, after several years of development, is an example of an infrastructure initiative aimed at strengthening digital sovereignty to enhance strategic autonomy from U.S. 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 crystallise 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 towards digital sovereignty.

Within BRICS, China is clearly a country enjoying both political stability and 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

[16] See https://ella.link/

digital self-sufficiency and enhancing the country's digital cyber-control, cyber-defence and offense capabilities. Importantly, Russia, China and other members of the Shanghai Cooperation Organisation (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 localisation provisions, which mandate the storage of personal data in servers located in the national territory (Shcherbovich, 2021). These policies laid the ground for the institutionalisation of the "Internet Sovereignty" discourse, articulated by Deputy Chairman of the State Duma Irina Yarovaya and consecrated into legislation in 2019, frequently dubbed as "Yarovaya Law" (Shcherbovich, 2021). Russia has dedicated considerable efforts to territorialise 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 to facilitate the control of information flows by Russian Internet Service Providers.

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 utilised the same measures that are branded as enhancing digital

[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)

[18] Here the term "digital infrastructure" should be considered as any physical and logical asset, i.e. 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.

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 not only been justified 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 U.S. 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 payment system established in 2014 to overcome total denial of e-payment service imposed on Russian banks by U.S.-based Visa and MasterCard. Previously, after the annexation of Crimea, U.S. 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 which is fully operated by the Russian National Card Payment System, a subsidiary of the Central Bank of Russia.

---

[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 judgements delivered in June 2020, criticised 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, Vladimir Kharitonov v. Russia) is offered by G. Grover and A. Thomas (2021)

[20] See the official website of Mir https://mironline.ru/ and its dedicated section on the website of the Bank of Russia https://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.

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 U.S. 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 Payment Interface (UPI) and the National Payments Corporation of India (NPCI), as well as the Digital India[22] programme. As we will argue in the following section, the ultimate goal of the latter plan is the development of a Digital Public Infrastructure 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 towards 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

[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" (2022).
[22] Digital India was launched in 2015. See https://www.digitalindia.gov.in/

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 like the BRICS. On the one hand, e-payments have been traditionally controlled by dominant U.S. providers such as Visa and Mastercard, 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 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.

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 U.S. 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

[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 analyse 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).

order is that the first mover advantage of WhatsApp – the use of which is subsidised to consumers by all Brazilian operators in the context of so-called "zero rating" schemes[25]—would have created "irreparable damages" to competition, 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 towards 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 digitalisation of the entire country through the development of digital public goods based on open source technology (Dattani, 2020). 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.

Resistance to Data Colonialism or Construction of Digital Protectionism?

Digitalisation 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

[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).

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 two decades ago.

Indeed, the Lula administrations of the 2000s realised 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 labelled 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 complexity in digital sovereignty discussions is the potential protectionist dimension. Indeed, 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.

Digitalisation 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 very cautious, understanding 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 U.S. 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 U.S. technology, as well as a situation of weakness in a global digital governance scenario dominated by Western actors' narratives. Clearly, in the Chinese authorities' view (Arsène, 2016), this situation called for an immediate and well-organised reaction, carefully blending policies, politics, and developmental approach to redefine Chinese digital sovereignty.

In 2014, China established the Cyberspace Administration of China (CAC) and the Central Commission for Cybersecurity and Informatisation, 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). The same year, the first World Internet Conference (WIC) was organised, creating a China-led global multistakeholder forum on digital governance. The first *Wuzhen Declaration*, proposed as a WIC outcome, featured "cyber sovereignty" in a prominent position amongst the advocated principles. 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 close attention to digital innovation. It is hoped through innovation Chinese researchers, developers, and ultimately the Chinese state could

achieve a sovereign position rather than relying on existing Western technologies, mainly from the U.S. Due to reduced production costs and increasing advancement in Chinese technology competitiveness, 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" strategy already in 2015, planned 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 centre 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 programmes, BRICS countries initiatives demonstrate that an equally – if not more – relevant preoccupation is the

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

preservation and expansion of the local digital economy while avoiding digital colonisation. However, understanding, planning, coherence, and implementation capabilities of each BRICS country vary enormously, spanning from a holistic Chinese approach to more fragmented or even unorganised 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 understanding the relevance of digital sovereignty and, chiefly, how to organise the concrete implementation of this multifaceted notion. However, not all BRICS countries, the individuals, the entities, and communities that compose them – or that we may find in most other countries around the world – may have the achieved the same understanding of this issues and, due to their reduced size, may not even be able to elaborate any measure to resist digital colonisation, even if they wished to do so.

In this context, Vashishta Doshi and Enrique Delgado's contribution to this volume reminds us that U.S. 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) that the U.S. maintains an upper hand in the technology field, exercises its digital sovereignty and expands this power globally. Reliant on U.S. digital infrastructures, middle powers like Brazil and India – as well as most other countries – find themselves in a situation of at least partial digital colonisation, 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, digitisation of public services, and establishment of Digital Public Infrastructure (DPI). The Indian government is not only aware of 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 so-called "zero rating"[27] practices where access to few dominant U.S. platforms such as Facebook was "offered" 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 enormously the dominance of a few commercial actors. Simultaneously these practices can considerably increase as 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 raise of 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, and perpetuate user dependency on such applications.[28]

We may fairly assume that, when the Indian government decided to prohibit the practices, one of the main goals was not only to preserve Internet openness, competition, and free expression. 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 enormously valuable insights and profits falling under foreign tax law, store user data in foreign servers, enhance foreign software and artificial intelligence development thanks to

[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).

such data, and sharing them with foreign intelligence agencies through numerous programmes unveiled by Mr Snowden.

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 colonisation 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 to exercise sovereignty over data (Belli, 2021a).

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; Belli, 2021b).

Members of the BRICS grouping are not only aware 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

[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

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” (Belli, 2017c), 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 entire populations that, frequently lack data protection frameworks to prevent undue exploitations. The indigenous populations are increasingly seen by the new digital colonisers 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 programme 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 capitalise on such a staggering expansion of connectivity infrastructure, Digital India fostered the creation of a set of APIs[31] commonly referred to as the “India

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)

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

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

Stack"[32] that play a key role in India's Digital Public Infrastructure, on top of which new home-grown digital services can be built.

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 acting as raw material to develop artificial intelligence 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 digitisation 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 artificial intelligence). When the software in question is not owned by the user, it is highly likely that in the long term the main beneficiary of such automations will be the software producer, i.e. 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

[32] See https://www.indiastack.org/

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 and more refined approaches to digital sovereignty. 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 colonisation of the country[33] by a corporation. That Facebook to date has been cooperating with U.S. intelligence agencies such as the NSA suggests President Rousseff's promotion of free-rating services can be now seen as a wilful 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 subsidieed nature of such apps, this

[33] It is important to stress that, despite multiple years of permissive attitude of Brazilian regulators towards 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.

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 concentrating all data collection. It is difficult to think that the Brazilian government does not realize that this 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 privatisation programme, 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 3 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 strategic assets in terms of digital sovereignty. While selling these corporations to foreign investors could generate juicy 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 on postponing the selling operation 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 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.

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, ultimately, in most countries subject to democratic elections, as Brazil, digital sovereignty policies are 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, 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 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.

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 recognises 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 African 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 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).

Conclusion: Digital Sovereignty Options

An agnostic approach to digital sovereignty in the BRICS acknowledges that different digital sovereigns may pursue self-determination, cybersecurity, power and control with different goals and outcomes. These leave us fundamentally with three options to structure digital sovereignty. The first one is 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 amongst themselves without necessarily communicate with the rest of the world – as some community networks do – or countries eager to build strong control on their national segment of the Internet, like China and Russia, but it can only be afforded in the long-term by those entities that can manage to be digitally self-sufficient an thrive while being relatively isolated.

The second option, which is ideal in the opinion of these authors, would be a shared global digital commons with rules to frame and regulate digital technologies and their uses in

a levelled regulatory playing field so that any entity would have an incentive to cooperate rather than engaging into antagonist behaviours. 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 organisations – 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 which share common – or at least (legally) interoperable (Belli & Zingales, forthcoming) – regulatory frameworks and technological tools. Such groups may limit information flows and technology exchanges with other blocs to the few sectors where shared agreement 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 towards 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.

This latter option seems particularly interesting for BRICS countries, in light of the grouping's recent commitment to enhance their cooperation on digital policy frameworks, with particular regard to cybersecurity issues. 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 testbed 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 an 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 and inclusion. This would 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 fulfil 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 Shanghai Cooperation Organization) 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 Ignacio 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.)

References

ACI Worldwide and Global Data (2022, April). *Prime Time for Real-Time Global Payments Report*. https://www.aciworldwide.com/real-time-payments-report

Andreessen, M. (2011, August 20). Why Software is Eating the World. *The Wall Street Journal*. https://www.wsj.com/articles/SB10001424053111903480904576512250915629460

Arsène, S. (2016). Global internet governance in Chinese academic literature: Rebalancing a hegemonic world order?. *China Perspectives*, 2, 25-35.

Ávila, R. (2018). Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. *International Journal on Human Rights*, 15(27), 15-28. https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/

Belli, L. (2011, November 7) *Internet governance v. Internet government*. MediaLAWS. https://www.medialaws.eu/internet-governance-v-internet-government/

Belli, L. (2015, April 20). *From Net Neutrality to Net Feudality*. MediaLAWS. https://www.medialaws.eu/from-net-neutrality-to-net-feudality/

Belli L. (2017a). Net neutrality, zero rating and the Minitelisation of the internet. *Journal of Cyber Policy*, 2(1), 96-122. https://doi.org/10.1080/23738871.2016.1238954

Belli, L. (2017b). Network Self-Determination and the Positive Externalities of Community Networks. In L. Belli (Ed.) *Community Networks: The Internet by the People for the People*: Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. FGV. https://www.intgovforum.org/en/filedepot_download/4391/1132

Belli, L. (2017c). *The scramble for data and the need for network self-determination*. OpenDemocracy. https://www.opendemocracy.net/luca-belli/scramble-for-data-and-need-for-network-self-etermination

Belli, L. (2021a). BRICS Countries to Build Digital Sovereignty. In L. Belli (Ed.). *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Springer-Nature. https://link.springer.com/chapter/10.1007/978-3-030-56405-6_7

Belli, L. (2021b). CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS. In L. Belli (Ed.). *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Springer-Nature. https://link.springer.com/chapter/10.1007%2F978-3-030-56405-6_1

Belli, L. (2021c). Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. *The African Journal of Information and Communication*, 28, 1-14. https://journals.assaf.org.za/index.php/ajic/article/view/12944

Belli, L. (2022). Structural Power as a Critical Element of Digital Platforms' Private Sovereignty. In Celeste, E., Heldt, A. and Iglesias Keller, C. (Eds). *Constitutionalising Social Media*. Hart. https://www.bloomsbury.com/uk/constitutionalising-social-media-9781509953707/

Belli, L. & Hadzic, S. (Eds). (2021). *Community Networks: Towards Sustainable Funding Models*. Official Outcome of the IGF Dynamic Coalition on Community Connectivity. Editora FGV. https://www.intgovforum.org/en/filedepot_download/92/20438

Belli L. & Zingales N. (forthcoming). Interoperability to foster open digital ecosystems in the BRICS. *Chinese Academy of Cyberspace Studies*.

Benyera E. (2021). *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data*. Routledge.

The Brazilian General Data Protection Law – Unofficial English version. (2020). CyberBRICS Project.

https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/

BRICS Conference – Central Bank Digital Currencies. 11 April 2022. [Video] https://cyberbrics.info/promoting-brics-economic-integration-via-central-bank-digital-currencies%ef%bf%bc/

BRICS. (2013). eThekwini Declaration and Action Plan. http://mea.gov.in/bilateral-documents.htm?dtl/21482

BRICS. (2015). VII BRICS Summit – Ufa Declaration. https://www.brics2021.gov.in/BRICSDocuments/2015/Ufa-Declaration-2015.pdf

BRICS. (2021). New Delhi Declaration. https://www.mea.gov.in/bilateral-documents.htm?dtl/34236/XIII_BRICS_Summit_New_Delhi_Declaration

Banco Central do Brasil. (2020, June 23). *Nova solução de pagamentos depende de prévia autorização do BC*. https://www.bcb.gov.br/detalhenoticia/17108/nota

Chander, A. & Sun, H. (2022). Sovereignty 2.0. *Vanderbilt Journal of Transnational Law, 53*(4), 283-324.

Couldry, N. & Mejias, U. (2018). Data colonialism: rethinking big data's relation to the contemporary subject. *Television and New Media, 20*(4), 336-349.

Creemers, R. J. E. H. (2020). China's conception of cyber sovereignty: rhetoric and realization. In D. Broeders & B. van den Berg (Eds.). *Digital Technologies and Global Politics*. Rowman & Littlefield. https://hdl.handle.net/1887/3220800

Dattani, K. (2019). "Governtrepreneurism" for good governance: The case of Aadhaar and the India Stack. *Area, 52*(2), 411-419.

Department of Communications & Digital Technologies. (2021). *Draft National Policy on Data and Cloud*. https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

Ding, J. (2018). *Deciphering China's AI Dream*. Future of Humanity Institute. https://www.fhi.ox.ac.uk/deciphering-chinas-ai-dream/

European Court of Justice. (16 July 2020). Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties*. https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en

The Economist. (2017, May 6). *The world's most valuable resource is no longer oil, but data*. https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

Escobar, P. (2019, August 19). BRICS was created as a tool of attack: Lula. *Asia Times*. https://asiatimes.com/2019/08/brics-was-created-as-a-tool-of-attack-lula/

Eyal, N. (2014). *Hooked: How to Build Habit-Forming Products*. Penguin.

Films and Publications Amendment Act 2019 – (English text signed by the President). (2019). https://www.fpb.org.za/about/legislation/attachment/films-and-publications-amendment-act-2019-english-text-signed-by-the-president-assented-to-19-september-2019/

Grover, G. & Thomas, A. (2021, February 22). Notes from a foreign field: The European Court of Human Rights on Russia's website blocking. *CyberBRICS*. https://cyberbrics.info/notes-from-a-foreign-field-the-european-court-of-human-rights-on-russias-website-blocking/

Huang, R. (2020, May 25). China Will Use Its Digital Currency To Compete With The USD. *Forbes*.

https://www.forbes.com/sites/rogerhuang/2020/05/25/china-will-use-its-digital-currency-to-compete-with-the-usd/?sh=3a85d7a131e8

Instituto Brasileiro de Defesa do Consumidor [IDEC] & Instituto Locomotiva. (2021). *Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E*. https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf

Jiang, M. (2019, June 3). U.S. Ban on Huawei: Superpowers' Insecurities and Nightmares. *CyberBRICS*. https ://cyberbrics.info/u-s-ban-on-huawei-superpowers-insecurities-and-nightmares/

Jiang, M. (2021). Cybersecurity Policies in China. In Belli, L. (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer-Nature, 183-226. https://link.springer.com/chapter/10.1007/978-3-030-56405-6_5

Judgment of 15 December 1983, BVerfGE 65, 1-71, Volkszählung

Lee, K.F. (2018). *AI Superpowers: China, Silicon Valley, and the New World Order*. Houghton Mifflin Harcourt.

Lessig, L. (2006). *Code: And Other Laws of Cyberspace Version 2.0*. Basic books.

Lobo, A.P. (2022, January 12). Câmara quer proibir vendas do Serpro e da Dataprev. *Convergência Digital*. https://www.convergenciadigital.com.br/Governo/Camara-quer-proibir-vendas-do-Serpro-e-da-Dataprev-59123.html

MacAskill, E., & Dance, G. (2013, November 1). NSA files: Decoded. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Mandl, C. & Versiani I. (2020, June 23). Brazil suspends WhatsApp's new payments system. *Reuters*.

https://www.reuters.com/article/us-brazil-central-bank-visa-mastercard-idUSKBN23V042

Ministry of Digital Development, Communications and Mass Media of the Russian Federation. (2015, May 15). *International Consortium for Development of New Mobile Operating System is Being Formed now*. https://digital.gov.ru/en/events/33225/

Ministry of Foreign Affairs of India. (2021, December 6). *India-Russia Joint Statement following the visit of the President of the Russian Federation*. https://mea.gov.in/bilateral-documents.htm?dtl/34606/India_Russia_Joint_Statement_following_the_visit_of_the_President_of_the_Russian_Federation

The National Archives. (n.d.) *Maps in time from 1900 to 2000*. https://www.nationalarchives.gov.uk/cabinetpapers/documents/maps-in-time.pdf

O'Donnell, F & Papa, M. (2021). India's multi-alignment management and the Russia–India–China (RIC) triangle. *International Affairs*, 97(3). https://doi.org/10.1093/ia/iiab036

Organization for Economic Cooperation [OECD] and Development and Inter-American Development Bank [IDB]. (2017). *Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit*. http://www.oecd.org/internet/broadband-policies-for-latin-america-and-the-caribbean-9789264251823-en.htm

Prashad, V. (2012). *Poorer Nations: A Possible History of the Global South*. Verso.

Presidência da República. (2023, January 2). *Despacho do Presidente da República*. Brazilian Government Official Gazette [Diário Oficial da União], Ed. 1-A, Section 1-Extra A, p. 7. https://www.in.gov.br/en/web/dou/-/despacho-do-presidente-da-republica-455351891

Razumovsky, D. (2022, July 14) BRICS: How Will the Organisation Get a ‘Second Wind’? *Valdai Club*. https://valdaiclub.com/a/highlights/brics-how-will-the-organisation-get-a-second-wind-/

Rousseff, D. (2013, September 24). Statement by H.E. Dilma Rousseff, President of the Federative Republic of Brazil, at the opening of the general debate of the 68th session of the United Nations General Assembly. *Voltaire Network*. https://www.voltairenet.org/article180382.html

Sanger, D. E. & Perlroth, N. (2019, June 15) U.S. Escalates Online Attacks on Russia’s Power Grid. *The New York Times*. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?smid=nytcore-ios-share

Shcherbovich, A. (2021). Data protection and cybersecurity legislation of the Russian Federation in the context of the “sovereignization” of the internet in Russia. In Belli, L. (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer-Nature, 67-131. https://link.springer.com/chapter/10.1007/978-3-030-56405-6_3

Strange, S. (1988). *States and Markets*. Continuum.

The South Commission. (1990). *The Challenge to the South: The Report of the South Commission*. Oxford University Press. https://www.southcentre.int/wp-content/uploads/2013/02/The-Challenge-to-the-South_HRes_EN.pdf

Vermeulen, J. (2022, March 1). Ramaphosa puts Internet censorship law into operation. *My Broadband*.

https://mybroadband.co.za/news/internet/435714-ramaphosa-puts-internet-censorship-law-into-operation.html

von der Leyen, U. (2020). *A Union that strives for more My agenda for Europe: political guidelines for the next European Commission 2019-2024*. https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf

World Bank. (2016). *World Development Report 2016: Digital Dividends*. http://pubdocs.worldbank.org/en/391452529895999/WDR16-BP-Exploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf

Xi, Jinping. (2015, Dec. 16). Speech at the 2nd World Internet Conference Opening Ceremony. https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony/

Zanolli, B. (2021). Reflections on Sustainability from a Quilombola Women Led Community Networks. In Belli, L. & Hadzic, S. (Eds). *Community Networks: Towards Sustainable Funding Models*. Official Outcome of the IGF Dynamic Coalition on Community Connectivity. Editora FGV. https://www.intgovforum.org/en/filedepot_download/92/20438

Zou, S. (2020, Dec. 16). Coding to be included in curricula. *The State Council of the People's Republic of China*. https://english.www.gov.cn/statecouncil/ministries/202012/16/content_WS5fd94001c6d0f72576941f60.html