Pre-print version of Min Jiang & Luca Belli. Contesting Digital Sovereignty: Untangling a Complex and Multifaceted Concept. 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*

Introduction

Contesting Digital Sovereignty: Untangling a Complex and Multifaceted Concept

Min Jiang[1]

Luca Belli[2]

University of North Carolina - Charlotte[1]

FGV Law School[2]

Abstract

This chapter lays the theoretical foundation for the book by disentangling the myriad discourse and interpretations of digital sovereignty from a Global South perspective. It argues that BRICS countries symbolize the "rise of the rest" in an increasingly multi-polar world, their digital policies critical to the future shape of global Internet and digital governance. In this book, the idea of digital sovereignty itself is viewed as a site of power contestation and knowledge production. Specifically, the chapter identify seven major perspectives on digital sovereignty in a complex discursive field: state digital sovereignty, supranational digital sovereignty, network digital sovereignty, corporate digital sovereignty, personal digital sovereignty, postcolonial digital sovereignty, and commons digital sovereignty. The chapter highlights the affinities and overlaps as well as tensions and contradictions between these perspectives on digital sovereignty with brief illustrative examples from BRICS countries and beyond. While a state-centric perspective on digital sovereignty is traditionally more salient especially in BRICS contexts, increasing public concern over user privacy, state surveillance, corporate abuse, and digital colonialism has given ascendance to an array of alternative perspectives on digital sovereignty that emphasize individual autonomy, indigenous rights, community wellbeing and sustainability.

Keywords: digital sovereignty, BRICS, Global South, Internet governance

Introduction

The last decade has witnessed a series of initiatives, both top-down and bottom-up, in BRICS countries (Brazil, Russia, India, China and South Africa) to reassert their digital sovereignty, especially in reaction to Snowden's 2013 revelations of NSA's massive surveillance programs. Brazil affirmed its commitment to building EllaLink, an undersea cable to connect Brazil directly to Portugal and by proxy connecting South America to Europe to circumvent U.S. surveillance and enhance its digital sovereignty. Putin's Russia, in a bid to restrict foreign influence and bolster its digital borders, pursued "sovereign RuNet" after passing the *Sovereign Internet Law* in 2019 despite grassroots resistance. In India, activists organized the social movement #SaveTheInternet in 2016, resoundingly rejecting Facebook's Internet.org initiative (which offers free limited web access to those who cannot afford it) as a form of anti-competitive digital colonialism. China, having long filtered content at the border with the Great Firewall and avowed to defend its digital sovereignty, ramped up its pursuit of digital independence in the unfolding US-China geopolitical rivalry, following Trump administration's ban on Huawei 5G products and threat to force a sale of TikTok to a U.S. firm in 2020. South Africa, like many other developing countries, tries to forge its own path of digital independence by leveraging Chinese tech equipment, U.S. digital platforms, and its newly enacted data protection policies. Across the five BRICS countries, digital sovereignty discourses, practices and policies have unfolded differently and unevenly.

This book project, the first of its kind to explore the digital sovereignty debate in the BRICS countries, attempts to untangle this complex and multifaceted concept from a Global South perspective. As a hotly debated topic, digital sovereignty inspires interpretive diversity and disagreements rather than uniformity and consensus (Broeders & van den Berg, 2020; Chander & Sun, 2022; Couldry & Mejias, 2019; Couture & Toupin, 2019; Duarte, 2017; Herlo, Irrgang, Joost, & Unteidig, 2021, Pohle & Thiel, 2020). The Westphalian notion of

sovereignty—nation-states accorded territorial integrity, legal equality and non-interference in international affairs monopolize the legitimate use of force and supreme authority over its territory—has not only been challenged in history repeatedly through episodes of colonial expansions and border transgressions (Krasner, 1999), but also faces unprecedented upset in the digital era from actors ranging from individuals and civil society groups to companies and supranational entities attempting to assert their power and control.

While the nation-state has traditionally been the legal vessel of sovereignty, chasms exist between normative assumptions of sovereignty and widely uneven practices in reality. Codified into the UN Charter, the modern system of nation-states can trace its origin to French philosopher Jean Bodin's conceptualization of sovereignty in the 16th century as well as the *1648 Peace of Westphalia* which created a group of legally equal states in the Holy Roman Empire (Grimm, 2015). Yet, centuries of colonization well after the Westphalia treaties and unilateral border transgressions (e.g. invasions of Iraq and Ukraine) call into question many a time the sanctity and norms of national sovereignty. Besides territorial infringements, asymmetric economic, political and cultural relations have throughout history produced foreign dominations and interferences. In addition, the normative assumptions of sovereignty also suffer from logical contradictions (e.g. non-intervention vs. democracy promotion) and lack of institutional arrangements to deter dominant actors from abusing their force unilaterally in international conflicts.

Sovereignty is frequently a function of power. Strong nation-states often engage in tactics beyond the scope of their sovereignty normatively defined; weaker states generally lack power and resources to exert effective influence, so much so that Krasner (1999) for instance, argues sovereignty is "organized hypocrisy". Further, an absolutist notion of sovereignty is criticized to be unattainable especially in an age of global challenges ranging from organized terrorism, regime change attempts, turbulent international financial markets

to global pandemics, climate change and digital technologies (Havercroft, 2011). In this perspective, the capability to muster digital technologies offers to a wide range of actors a new powerful tool to exercise self-determination[1], control and ultimately sovereignty.

For this project on "digital sovereignty", we depart from a conventional, normative, state-centric approach towards sovereignty that has dominated academic, public and policy debates. In reality, borders are repeatedly transgressed and international norms are frequently violated. The gap between the norms of state sovereignty and reality is especially pronounced in the digital realm where much of the world's digital infrastructure, data and service is overwhelmingly dependent on a handful of Silicon Valley firms and increasingly their Chinese counterparts. By re-framing "digital sovereignty" as contested rather than merely accepted, discursively practiced rather than legally binding (Couture & Toupin, 2019; Pohle & Thiel, 2020), we make room for exploring the concept at levels beyond the default plane of nation-states, allowing scholars, policymakers, and the public to engage with a wider range of perspectives and discourses on digital sovereignty that can provide visions for the future, especially beyond U.S. and Chinese influence in global digital affairs and governance.

---

[1] The right to self-determination plays an instrumental role to allow individuals to enjoy their inalienable human rights. For this reason, it is enshrined as the first article of both the *Charter of the United Nations* and the *International Covenants of Human Rights*. According to these international legal instruments, states have agreed that "all peoples have a right to self-determination" and that "by virtue of that right they are free to determine their political status and to pursue their economic, social and cultural development." While self-determination is usually discussed in its external dimension, i.e. territorial and political independence from external actors, it is essential to stress that here we are referring to 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 is also corroborated by the fundamental right to "informational self-determination" as an expression of the human right to have and develop a personality, first recognised by the German Supreme Court, in the 1983 Census case. The fundamental right to free development of personality is formally recognised internationally. Article 22 of the *Universal Declaration of Human Rights* affirms that "everyone is entitled to the realisation of the rights needed for one's dignity and the free development of their personality," while the *International Covenant on Economic, Social and Cultural Rights* consecrates this fundamental principle regarding the right of everyone to education and to participate in public life. Particularly, the Covenant's signatories have agreed that the right to education "shall be directed to the full development of the human personality and the sense of its dignity [...] and enable all persons to participate effectively in society" (Article 13.1). Moreover, the free development of personality is explicitly considered as instrumental to exercise the fundamental right "to take part in cultural life [and] to enjoy the benefits of scientific progress and its applications" (Article 15) (Belli, 2017; 2019).

Digital sovereignty is ultimately the exercise of power and control over digital infrastructure, data, services, and protocols (Floridi, 2020). Although it is customary to approach "digital sovereignty" from a state-centric perspective, this orthodox approach tends to ignore the alternative perspectives and claims to digital sovereignty made at the grassroots and supranational levels as well as at the intersections between them (Couture & Toupin, 2019). For instance, although the Russian state under Putin's government is known for promoting an ultra-nationalistic version of "Internet sovereignty" aimed at separating the RuNet from the global Internet, it also routinely faces grassroots resistance with individual and collective expressions of digital sovereignty (Daucé & Musiani, 2021). While U.S. tech giants wield immense sovereign-like power across the globe, thus exporting U.S. state sovereignty by proxy (Belli, 2022), they have also been challenged by individuals such as data activist Maximilian Schrems in the European Court of Justice (Chander, 2020) as well as bottom-up social movements and connective actions (Bennett & Segerberg, 2013) such as India's #SaveTheInternet movement that rejected Facebook's Internet.org initiative seen as a form of digital colonialism (Mukerjee, 2016). The BRICS grouping, although initially an eclectic network of emerging economies interested in multilateral trade, is also increasingly cooperating on digital development and policymaking (Belli, 2020), taking a loosely coordinated approach in contrast to EU's more uniform supranational stance towards "digital sovereignty" (Leonard & Shapiro, 2020), for instance, through GDPR.

By problematizing "digital sovereignty" and moving beyond a state-centric conceptualization, we can start to raise fundamental questions as to who (legitimately) wields power and control over digital infrastructure, data, services, and protocols; who ultimately defines "digital sovereignty" and for what purposes; and to what extent a particular form of "digital sovereignty" enhances or worsens the autonomy of, choices by and protection for a country's citizens. Unlike the freewheeling cyberspace dreamed up by Barlow (1996), we

recognize cyberspace is not at all free from states, rules, barriers, prejudices, competing interests or power differentials. While there is a tendency to frame Western conception of digital sovereignty in terms of public interest and democratic values and conversely brand BRICS promotion of the concept as protectionist and authoritarian, there is also a long history of state surveillance programs in both democratic and nondemocratic countries alike (Chadwick, 2006). While the legitimacy of authoritarian states to exercise "digital sovereignty", for instance to censor, is often called into question, the Snowden revelation of the far reach of NSA and its "Five Eyes" partners into global networks also casts doubt on some Western democracies' legitimacy and neutrality, especially when their actions contradict the purported principles of territorial integrity, legal equality and non-interference.

If the nation-state is no longer the only legitimate actor with the ability to exercise power and control in cyberspace or is even capable of doing so in certain cases, it is then possible and desirable to look past the normative, idealistic, and often mythical state-centric construction of "digital sovereignty" and start to understand, describe and assess how digital sovereignty is structured in practice. Non-state actors and the exercise of their sovereignty would enter the picture: "corporate sovereignty" embodied by the likes of Google, Facebook, and Amazon whose almighty power easily eclipses those of small nation-states (MacKinnon, 2012); "personal digital sovereignty" grounded in individual rights, autonomy and freedom in relation to body politics and individual personhood (Koopman, 2019); "postcolonial digital sovereignty" aimed at challenging the violent dispossession of (digital) resources in the process of (digital) colonization (Couldry & Mejias, 2019; Coulthard, 2014); and "commons digital sovereignty" motivated by a desire to create alternatives to state or commercial digital technologies to achieve self-determination and sovereignty of the people through technology managed as a common good (Belli, 2019; Haché, 2017). These diverse ideas challenge the singular, normative assumptions of digital sovereignty centered on the nation-state.

Collectively, this project shines a spotlight on how different types of digital sovereigns besides governments can claim sovereignty and exercise their power over digital infrastructure, data, services, and protocols in BRICS countries. While these developing countries are playing an increasingly important role in global technological development and digital policymaking, their conceptions, narratives and initiatives of digital sovereignty remain surprisingly under-studied. Contained here is an excellent collection of cutting-edge academic analyses of key digital sovereignty issues in the BRICS countries—ranging from historical imaginaries to up-to-date conceptualizations of digital sovereignty, from payment systems to smart cities as architectures of digital sovereignty, from legal analysis to empirical accounts of the exercise of digital sovereignty by states, companies and communities—offering much needed visibility to frequently neglected perspectives from the Global South.

Further, these BRICS countries present highly relevant and intriguing case studies of digital sovereignty from the Global South with a considerable range. In the BRICS bloc, one finds not only extreme hostile countries like Russia centralizing its Internet control and manipulation in service of its ongoing war efforts in Ukraine, but also a tech powerhouse like China now locked in a new geopolitical rivalry with the U.S. Besides, India and Brazil—both relatively new democracies with some recent regress in democratic governance—are crucial middle-power countries with the potential to reshape the digital landscape not only in the Global South but also exert influence globally. Finally, South Africa represents a digital arrangement many other countries increasingly find themselves in, i.e. relying heavily on China for cheap hardware, the U.S. for applications/software, and its own newly enacted data protection laws to navigate the unfolding digital spaces. Taken altogether, BRICS countries offer a wide range of digital sovereignty policies and solutions from the Global South.

In the following, we provide an account of why an exploration of the digital sovereignty debate in the BRICS countries is particularly important and relevant at this moment in time. We outline seven major theoretical perspectives on digital sovereignty that serve to elucidate the different digital sovereigns operating on different planes. We close this introduction with a summary for the chapters that compose this volume to recognize their connections and valuable contributions to the digital sovereignty debate in BRICS countries.

Why BRICS?

Goldman Sachs economist Jim O'Neill first coined the term "BRIC" (O'Neill, 2001) to designate the four largest emerging economies—Brazil, Russia, India and China—that experienced a similar phase of development. Geographically dispersed, economically distinct, culturally diverse, and politically different, BRICS countries may not appear to be the most coherent motley crew (Sparks, 2014), especially given the multiple economic, political and territorial disputes among them as well as the multifold impact of the pandemic on the BRICS countries and their diverging opinions regarding the ongoing war in Ukraine. As a loosely joint bloc that does not impose binding conditions on its member states, BRICS's informality and low degree of institutionalization signal the bloc's unwillingness to directly challenge the existing U.S.-centered Western global order (Stuenkel, 2020). Rather than being overtly anti-West as Putin's Russia turned recently, other BRICS member states are more "non-Western," in pursuit of support and expanding influence in the existing structure.

Geopolitically, emergence of the BRICS countries represents the "rise of the rest" in a post-Western, increasingly multipolar world (Stuenkel, 2016). The U.S., as the world's sole superpower since the end of the Cold War, suffered a decline in relative power following several pivotal episodes in recent decades: the highly costly and unpopular wars in Iraq and Afghanistan for two decades since 2001; the 2008 global financial crisis; the pandemic-induced recession since 2020. BRICS countries, on the other hand, include some of

the world's largest growth engines (see Table 1), representing 25% of global GDP, 42% of the world's population or 3.2 billion (CGTN, 2022), and 44% of the global Internet population[2]. Even the impact of the Ukraine war on Russia has been less severe as expected (Tan, 2023). BIRCS symbolizes a slow changing global order where the U.S.'s relative decline has paved the way for emerging powers like China, India, Brazil, Russia and South Africa from the Global South.

Table 1: BRICS Countries Profiles (Compared to the U.S.)[3]

	Brazil	Russia	India	China	South Africa	U.S.
Population (2022)	215 million	146 million	1403 million	1448 million	60 million	334 million
Internet Population (2022)	168 million	115 million	658 million	1051 million	41 million	311 million
GDP (2020, USD)	$1.44 trillion	$1.48 trillion	$2.66 trillion	$14.72 trillion	$0.34 trillion	$21 trillion
GDP (2021, USD)	$1.61 trillion	$1.78 trillion	$3.18 trillion	$17.73 trillion	$0.42 trillion	$23.32 trillion
GDP (2022, USD)	$1.89 trillion	$2.13 trillion	$3.47 trillion	$18.32 trillion	$0.44 trillion	$25.04 trillion
GDP per capita (2021, USD)	$7,507	$12,195	$2,257	$12,556	$7,055	$70,249

Sources: WorldoMeter (2022) for population figures, Statista (2022) for Internet population figures, World Bank (2021) for 2021 GDP and GDP per capita figures, IMF (2022) for 2022 GDP figures.

Economically, the BRICS grouping, an unorthodox experiment, is also a direct response to the 2008 global financial crisis and the subsequent 2009 Eurozone crisis that exposed the instability of the global financial system centered around the U.S. The initial BRIC grouping organized their first ad hoc informal gathering in 2006, prior to the UN General Assembly. Right after the 2008 global economic crisis, the BRIC countries whose economies were largely spared from the crises convened their first summit in 2009 with the

[2] Even though some BRICS countries such as China's aging population and declining birth rate pose considerable challenges to its long-term sustainable development (Bai & Lei, 2020).

[3] Note that 2022 GDP figures were estimates by IMF released in October 2022. Russia's economic statistics are subject to considerable variations due to war-related sanctions and shrinkage since February 2022. Russia's federal statistics service announced a 2.1% GDP contraction for 2022, reported Business Insider (Tan, 2023). It is lower than IMF's GDP estimate for Russia, but better than 8.8% to 12.4% contraction projected in April 2022. Many acknowledge Russia's economy has been resilient due to gains in energy prices.

induction of South Africa in 2010. The grouping's cooperation, cemented by the establishment of the New Development Bank in 2015 with $100 billion initial capital and Contingent Reserve Arrangement, has come a long way. The New Development Bank, conceived not as a rival to established financial institutions such as the IMF and the World Bank, creates a parallel financial system for the developing countries and symbolizes their expectations and aspirations (Economic Times, 2015). In 2021, the New Development Bank added UAE, Bangladesh, Uruguay and Egypt as new members (NDB, 2022). In 2022, the BRICS bloc took on a BRICS+ format hoping to extend the potential partnership to Indonesia, Argentina, and Nigeria and more (CGTN, 2022).

In digital matters, during a time of deep economic crisis, widespread social upheaval, and unprecedented nativist furor, the BRICS grouping provides pointers to the future shape of a new global (digital) order. The war in Ukraine marked the most significant military conflict, including cyberwarfare, in Europe since WWII. Except the Putin administration bent on restoring its sphere of influence in the former Soviet states and mounting a direct challenge to the U.S. as a global superpower (Hinck, Cooley & Kluver, 2019), China and other emerging powers seem more interested in rising *alongside* the U.S. without either assimilating into the current Western-centric global order or directly challenging it (Barma, Ratner & Weber, 2014). Instead, they have been creating a "parallel order" (Stuenkel, 2016) to accommodate and complement existent international institutions while making more room for their own autonomy and ability to bargain, compete and mitigate risks associated with dependence on external products or services in an increasingly multipolar world. China, for instance, has developed over the last 25 years the only digital ecosystem to rival Silicon Valley's in both scale and sophistication (Miao, Jiang & Pang, 2021). India has also built a whole set of Digital Public Infrastructure (DPIs) for identity, payments and data exchange that offer an

alternative framework for the private sector-led platforms created by either the U.S. or Chinese firms (see Hariharan & Natarajan's chapter in this volume).

Russia's invasion of Ukraine in 2022 puts its BRICS partners in a difficult bind. The BRICS bloc, notably China, endorses territorial sovereignty. Ten days after the war started, the BRICS-led New Development Bank stopped all new transactions in Russia, signaling its willingness to avert risks (USCC, 2022). Yet, as the war dragged on and motivated by self-interest, the BRICS bloc did not impose on Russia the same sanctions as the U.S. and EU did, citing NATO expansion as a legitimate security concern (CNN, 2022). Instead, despite clear divergence of opinions on the war, the group tried to maintain neutrality and continued with the annual BRICS meeting (USCC, 2022). The 2022 BRICS summit reiterated the grouping's commitment for intra-BRICS cooperation focused on sustainable development towards building a global order more favorable to developing countries to address issues including food insecurity, energy shortage, inflation, debt crisis and de-dollarization (CNN, 2022).

Ultimately, the war in Ukraine has not changed BRICS countries' trajectory to explore alternative paths for economic and social development that do not depend on the U.S.-dominated international order that has failed to eradicate—and frequently condoned or produced—gross inequalities, dysfunctional democracies, environmental catastrophes and persistent militarism. While it is possible that mounting civilian toll, nuclear threat as well as worsening energy, food and economic crises worsened by the ongoing Ukraine war could tip the balance for Russia's BRICS partners, the bloc will likely move forward while preserving multilateral and—most importantly—trade relations critical to their own interest and the functioning of their economies and societies (Zondi, 2022).

Seen from a Global South perspective, the BRICS is the latest iteration of a much wider trend towards "South-South cooperation" (The South Commission, 1990). The concept

of Global South entails complex layers of geographical, historical, cultural, political and economic meanings (Lumumba-Kasongo, 2015). While "Global South" traditionally refers broadly to the regions of Africa, Asia, and Latin America as loci of underdevelopment and cultural primitivism in contrast to the "advanced" societies of North America and Europe in a postcolonial sense, the phrase has also signified over time "center-periphery" dynamics in geopolitical power relations (Dados & Connell, 2012). Historically, anticolonial movements have found expressions in the League Against Imperialism begun in 1928 as well as the Non-Aligned Movement started in the 1950s involving 120 countries to counterbalance the U.S. and Soviet power blocs during the Cold War. It was from such historical lineages that one can trace the Group of 77 formed in the 1960s, Group of 15 in the aftermath of the Cold War and the BRICS after the 2008 global financial crisis (Prashad, 2012). From a postcolonial perspective, BRICS symbolizes a continuation of a centuries' old attempt to challenge and change an unfair system that preserves former colonizers' interests and gain independence.

Further, beyond the postcolonial lens, the emergence of the Global South, and BRICS in particular, signifies a "*post*global" moment when the world's subalterns recognize the U.S.-led neoliberal globalization experiment as a failed master narrative (Lopez, 2007, p.1). Instead of seeing globalization and trickle-down economics lift all boats, the last four decades saw the poor, the marginalized and the disenfranchised bore the brunt of the suffering. Crisis after crisis—from the 1998 Asian financial crisis to the dot-com bubble, from 9/11 to the ensuing 20-year war on terror, from the 2008 financial crisis to the current pandemic-induced global recession—traditional Western-led financial and governance institutions, notably the International Monetary Fund and World Bank, are often perceived in the Global South increasingly as barriers rather than propellers of economic and human development. While Russia is not typically considered part of the Global South given its previous super power

status and its complicated relations with other developing countries, its membership in the BRICS bloc represents a repositioning of Russia's strategic interest and alliance vis-à-vis the West. It is within such historical contexts that the BRICS have led the search for a "post-Western" model of global governance.

Finally, whether "post-Western" or "non-Western", BIRCS' default preference, unlike Russia's in retrospect, is evolution rather than revolution (Armijo & Roberts, 2014). As beneficiaries of the global system, BRICS members (China and India in particular), may find it both hard and costly to abolish the existing global order and establish new ones. So, while President Trump attempted to weaken the existing rules and norms of the global system including the WTO and Paris climate accord, BRICS member countries have more invested interest in preserving them. Moreover, it seems that BRICS countries', especially China's, vision or capacity to create new systems and institutions such as the Belt and Road Initiative may not only lack intellectual foundation, but also face mounting pushbacks and constraints from within the existing system between a rising power and a ruling one (Allison, 2017). Instead, BRICS countries have opted for a type of "competitive multilateralism" (Stuenkel, 2020) that allows them to flexibly choose political and collaborative frameworks to maximize their national interest. Even though BRICS countries may not speak for or represent the diverse voices and regions of the Global South, its emergence and heterogeneity do mark a crucial moment of international development that is worth unpacking and examining.

Building Digital Sovereignty "BRICS by BRICS"

Just as the BRICS are the developing world's response to the instability and unfairness of a globalized economy, many of the BRICS "digital sovereignty" initiatives are also expressions of a strong inclination to seek independence from a U.S.-centric model of digital development, perceived as unfair and unsustainable. While "digital sovereignty" is never explicitly mentioned in official BRICS documents, with 40% of the world's population

and large sums of one of the world's most valuable resources—personal data (The Economist, 2017), BRICS countries are increasingly leveraging their positions to develop digital technologies, economies and policies.

Although the "free-flow-of-information" narrative supported by Western countries and championed by the U.S. is appealing, one must acknowledge that global data flows have grown in highly asymmetric fashions. Data has been extracted from Global South countries to generate value mainly in the U.S. while simultaneously rendering the Global South increasingly dependent on technologies provided by a handful of typically U.S. companies. In this context, joint partnerships and activities dedicated to digital affairs and technological cooperation started to appear in the BRICS grouping's strategic agenda over time. Post-Snowden, the 2015 BRICS Summit issued the *Ufa Declaration* to establish a working group on the security of ICT use with the aim "to develop practical cooperation with each other in order to address common security challenges in the use of ICTs" while "sharing information and case studies on ICT policies and programs" (Indian Ministry of External Affairs, 2015).

In the same year, BRICS ICT ministers signed the *Memorandum of Understanding on Cooperation in Science, Technology, and Innovation* to promote digital initiatives such as the BRICS Digital Partnership, the BRICS Partnership on New Industrial Revolution (PartNIR), and the Innovation BRICS Network (iBRICS Network). In 2021, the *New Delhi Declaration* jointly issued at the 13th BRICS explicitly called for—the first time in 15 years—the establishment of "legal frameworks of cooperation" on crucial issues such as "ICTs development and security" (Indian Ministry of External Affairs, 2021). Issues of data protection, cybercrime, content regulation and e-commerce also received prominent attention.

BRICS's exploration of alternative modes of digital development, governance and regulation is shaped by several epoch geopolitical events, chief among them: Snowden's

2013 revelations of NSA's global surveillance program, the vulnerability of democratic infrastructures to social media-enabled manipulation epitomized by the 2016 U.S. presidential election, Russia's invasions of Ukraine in 2014 and 2022 and the subsequent need to cope with Western-imposed sanctions. While China has been systematically grafting borders onto the Internet for decades for fear of a "color revolution", many countries around the world were jolted by these events to move away from a "deterritorialized" view of the Internet towards one that is "territorialized" and "sovereignty-minded". Russia's invasion of Ukraine has further prompted the creation of digital curtains on the Internet, with the EU requesting to block Russian state media on TikTok, Facebook and Microsoft (Bond, 2022), and Russia blocking access to Western social media.

As a result, we are witnessing strong currents of territorialization and renationalization of the Internet, extending to infrastructure, data, hardware, software, platforms and tech standards. BRICS countries are no exceptions, although their aims and strategies may be remarkably different. After Snowden revelations, Brazil passed the *Brazilian Civil Rights Framework for the Internet*, or *Marco Civil da Internet*, its first law to create rules and obligations in the Internet environment. In this example, asserting national sovereignty online is not only compatible with human rights and rule of law, but can also enhance participatory democracy. Russia, on the other hand, not only approved data localization in 2015 and the *Sovereign Internet Law* in 2019, but also developed infrastructural capabilities to disconnect the Russian segment of the Internet "RuNet" from the global Internet (see Bronnikova et al. chapter in this volume), which in retrospect appears to be a strategy to build resilience from Western sanctions and advance Kremlin's aims.

Following an ambitious Digital India plan aimed at fostering digital inclusion and transformation, India banned zero rating practices in 2016 on the ground of net neutrality to avoid what is perceived to be a disguised form of digital colonialism (Mukerjee, 2016).

Moreover, after GDPR went into effect in 2018, India has also been mulling over its Personal Data Protection Bill that is now inching towards passage with data localization provisions (National Law Review, 2022). On the other hand, China elevated "Internet sovereignty" and cybersecurity to a national priority. The Cyberspace Administration of China (CAC), headed by President Xi Jinping himself, was established in 2014, followed by numerous Internet legislations and policies including its 2017 *Cybersecurity Law*, *Personal Information Protection Law* and *Data Security Law* in 2021 (Jiang, 2020). South Africa, like many African countries, not self-sufficient in technological development which make them reliant on U.S. platforms, Chinese tech equipment, and European digital legislation model, are nevertheless designing data protection policies with the unintended effect of increasing state control over private communication (see Calandro chapter in this volume).

These state-led nation-building efforts, however, are not the only developments that define "digital sovereignty" in BRICS countries, for after all what is sovereignty without the autonomy, choice, or freedom of its own citizens? (Fuchs, 2015). Brazilian users' participation in Mastodon, a decentralized federated social media platform, points to the use of commons-inspired practices of digital sovereignty as an alternative to dominant, privatized, profit-oriented social media (see Tomaz's chapter in this volume). In the Russian case, as intimidating as surveillance and censorship may seem, they are never complete with limited spaces for resistance and evasion (see Bronnikova et al. chapter in this volume). Often seen as totalitarian by Western observers, the Chinese Internet is far from being uniform, obedient, or frictionless. In 2019, for example, a Chinese professor sued Hangzhou wildlife park over facial recognition data collection without his consent, for which the court ordered the park to delete his data and awarded him a partial compensation of $158 (CGTN, 2021). Cases as such represent individual and community desires for privacy, autonomy, and self-determination that make up a key part of digital sovereignty discourses.

It is also widely recognized BRICS nations have a highly-mixed record of digital authoritarianism and very heterogeneous use of cyber capabilities to assert sovereignty through offensive or defensive actions. While Russia's RuNet goes to the far extreme of "digital isolation" (Sherman, 2021), the Chinese state is known to operate extensive domestic surveillance programs and is frequently cited as a likely originator of many cyberattacks on external targets (Arsène, 2016). New democracies like Brazil and India have also experienced notable regress in civil liberties and restrictions of digital rights under Bolsonaro's and Modi's governments (See Thumfart's chapter in this volume). South Africa's securitization discourse is similarly worrying for legitimizing state surveillance reminiscent of the apartheid police state (Kuehn, 2018). Far from being an immaculate source of inspiration and emulation, BRICS digital initiatives for online safety and cybersecurity can often seem as pretexts for surveillance and censorship.

Yet the tendency to lump BRICS nations into an authoritarian camp under a "democracy vs. authoritarianism" new Cold War framework is far too simplistic and conflict-prone by assuming Western countries are immune from surveillance or censorship. Rather, BRICS states' surveillance and censorship practices need to be held in juxtaposition to the grouping's legitimate anti-imperialist, anti-colonial desires, analyzed situationally. Dependence on foreign, especially U.S., digital technologies, platforms, and services can create and has created conditions of digital neo-colonialism that combines surveillance capitalism (Zuboff, 2019) and data colonialism (Couldry & Mejias, 2019). The "free" addictive services offered by dominant U.S. platforms are extractive instruments of data mining in building a new form of indentured labor that perpetuates economic and digital dependence (Avila Pinto, 2018). Overtime, "the BRICS grouping is increasingly aware of the economic opportunities brought by digital technology but also that "free" digital services provided by foreign corporations are not free. They are paid with one of the most precious

national assets—i.e. data—and, ultimately, with national sovereignty" (Belli, 2021b, p.282). Such complex dynamics would not have been captured by an all-encompassing, categorical "democracy vs. authoritarianism" Cold War framework in the digital field.

To further complicate the anti-imperialist, anti-colonial narrative in the digital sovereignty debate are questionable digital practices within BRICS countries and conflicts between them (Fuchs, 2015). While U.S. firms' extractive activities are the subject of postcolonial critique, there is no denial domestic BRICS companies have often benefited from the exclusion of foreign competitors. For instance, not only do large Indian tech companies such as telecom firm Reliance Jio gain valuable access to domestic user data, but data localization measures may well transfer power from foreign tech giants to domestic elites instead of instituting data policies that foster citizens' data sovereignty, as a public good of the people, by the people, for the people (Kovacs & Ranganathan, 2019). Tensions also exist between BRICS partners over their digital policies. China's neo-mercantilist expansion around the world, for instance, has met with both successes and failures (French, 2015). While Huawei and ZTE have offered low-cost, high-function handset solutions to many poor developing nations, Huawei's digital initiatives may well create new forms of digital dependence (See Calzati's chapter in this volume). In a more contentious episode, India banned 59 Chinese apps in 2021 following its border clash with China, with an additional 54 added to the list in 2022 (Reuters, 2022).

Aware of such complex and multifaceted contexts, we argue that the quest for digital sovereignty to exercise power and control over digital infrastructure, data, services, and protocols is pursued by a plethora of actors beyond just the nation-states. They include empowered individuals, companies, communities, and even supranational alliances. Rather than following a linear inquiry on a topic as complex as digital sovereignty focused on nation-states only, it benefits to unpack its complexity that unfolds on different planes, in

different domains, and across BRICS countries. Doing so will avoid making nation-states the default actors with the legitimacy or capacity to exercise digital power and control over citizens' data and digital lives. As judged by the short yet intense history of the Internet, nation-states routinely fail to protect their citizens' digital rights and aspirations for self-determination. Only by asking to who can (legitimately) wield power and control over digital infrastructure, data, services, and protocols; who ultimately defines "digital sovereignty" and for what purposes; and to what extent a particular form of "digital sovereignty" enhances or worsens the autonomy, choices and protection of a country's citizens can we start to have a more meaningful debate of "digital sovereignty".

Perspectives on Digital Sovereignty

Given the plurality of discourses surrounding "digital sovereignty", we map out here seven major perspectives instead of assuming nation-states are the default and ultimate holders and arbiters of digital sovereignty. Not only does this approach acknowledge the important roles nation-states play in structuring digital infrastructure, data, services, and protocols within their borders, it also recognizes the complicated realities in exercising digital sovereignty. We include in our conceptual mapping: state digital sovereignty, supranational digital sovereignty, network digital sovereignty, corporate digital sovereignty, personal digital sovereignty, postcolonial digital sovereignty, and commons digital sovereignty (see Table 2). A myriad of actors—governmental policymakers, technologists, activists, individuals, indigenous and local communities—approach "sovereignty" from different perspectives, with unique assumptions about social justice, autonomy and governance. In the following, we briefly explicate each perspective, related core concepts, their similarities, and differences as well as their applications in BRICS countries and beyond.

It is worth to note that the applications of these perspectives are highly contextual. For instance, while a BRICS or non-BRICS country's government can pursue state digital

sovereignty, it can also take on a more corporate, postcolonial or commons perspective depending on the specific circumstances. Thus, while the Indian government initiated the ban of dozens of Chinese apps including TikTok to exercise its state sovereignty to protect domestic Internet companies and the data sovereignty of its own citizens, it can also push for the creation and repository of digital public goods among BRICS and other developing countries, a move that is more aligned with a commons digital sovereignty framework. On the other hand, various civic groups may also articulate from any of the seven digital sovereignty perspectives outlined including the ones that support or oppose state regulation of cyberspace. In a word, actors including nation-states face different policy choices.

The application of digital sovereignty within specific domains ranging from data and algorithm to smart cities and community networks can also be complicated by the specific digital sovereignty perspectives the ground the specific application. For instance, it is possible to conceive of "data sovereignty" as a domain of national laws and governance structures (Lukings & Lashkari, 2022), thus grounding discussions of "data sovereignty" in a state-centric perspective. However, data can also be regarded as a sphere of individual freedom and personhood (Koopman, 2019) to be protected from state surveillance (Epstein, 2016), making discussions of "data sovereignty" comport with a personal digital sovereignty perspective. Similarly, "algorithmic sovereignty" may regard algorithms as scientific, neutral and sovereign in their own right, which aligns with a network digital sovereignty perspective. Conversely, "algorithmic sovereignty" can also be positioned to wield corporate power (Jiang, 2014) or become an extension of state oversight of artificial intelligence in the case of China's new registry for recommendation algorithms (Sheehan & Du, 2022). Still others may argue that "algorithmic sovereignty" should be inclusive, transparent, bottom-up, and community-based, allowing communities to exercise power and control over fundamental digital protocols and infrastructures (Reviglio & Agosti, 2020; Roio, 2018). Given the

proliferation of the discourse of sovereignty in many digital domains and applications, it is important to recognize the particular theoretical perspectives from which actors and interlocutors evoke that carry unique assumptions, biases and implications.

Table 2. Perspectives and Applications of Digital Sovereignty in BRICS Countries

BRICS	**Theoretical Perspectives**	**Core Concepts**	**Applications**
Brazil **R**ussia **I**ndia **C**hina **S**outh Africa	State Digital Sovereignty	State regulation of digital infrastructure, data, information flow, access, user rights; defense of cyber borders; digital independence; digital nationalism	Data, Algorithms, Undersea cable, Telecom networks (5G), Cloud services, Smart cities, Electronic payment systems, Digital currencies, Social media, Community networks, …
	Supranational Digital Sovereignty	Negotiated interdependence between states to assert digital power and control; framework of digital cooperation; collective state actions and digital cooperation bodies	
	Network Digital Sovereignty	Network interoperability; neutrality of networks; undesirability of state regulation; borderless cyberspace; cryptocurrency	
	Corporate Digital Sovereignty	Laissez-faire, private ordering, and tech giant self-regulation; government regulation as unwelcomed unless it supports tech giants' interests; surveillance capitalism	
	Personal Digital Sovereignty	Informational self-determination, autonomy; individual rights, digital personhood; self-sovereign identity; security and privacy by design	
	Postcolonial Digital Sovereignty	Voice and rights of indigenous peoples; post-colonialism, freedom from (neo)colonialism; access, possession, ownership, control of digital resources	
	Commons Digital Sovereignty	Network self-determination; free and open-source software; freedom from corporate and state control; data cooperatives; digital public goods	

State Digital Sovereignty

Normative assumptions of sovereignty—territorial integrity, monopolistic use of force, legal equality, and non-interference in international affairs—have been seriously challenged by the advent of the cyberspace based on a global network of networks (Lessig, 1999). Over time, however, many governments have re-asserted their power (Goldsmith &

Wu, 2006). Laws and policies regulating how digital technologies could be used at the national level have been passed since the mid-1990s, implemented through Internet intermediaries who act as "points of control" (Zittrain, 2003) such as operators of national telecom infrastructure, cloud services, domain name systems, hardware manufacturers, etc. Overall, discourses of state digital sovereignty concern government authority and legitimacy as well as their ability to regulate and control digital infrastructure, data and users to maintain effective national laws and achieve varying degrees of autonomy or independence.

Over the past three decades, BRICS nations have been strong advocates of state digital sovereignty. China was among the first to graft borders back onto the Internet in the 1990s through mechanisms like the "Great Firewall" to filter content and maintain national ownership of digital infrastructure (Jiang, 2010). Today, it has the only digital ecosystem that can rival Silicon Valley's, fueled by a degree of technological nationalism to produce indigenous technologies (Jiang & Fu, 2018). China's articulation of cyberspace sovereignty serves as a justification for rejecting foreign interference in its information environment as well as establishing the dominance of party-state ideology and indigenous capacity to innovate (Creemers, 2020; Fang, 2018). In the aftermath of Google's high-profile exit from China, "Internet sovereignty" was adopted as an official state policy by the Chinese government in 2010 to assert control over its infrastructures, information and population (Jiang, 2020). This approach was furthered strengthened and promoted abroad by Xi's administration in response to the 2013 Snowden revelations. The "sovereignization" of the Russian Internet leveraged the scandal to legitimize the Kremlin's approach to controlling RuNet activities (Nocetti, 2015). Following the passage of *Sovereign Internet Law* in 2019, Russia developed its own technical work-around and alternative version of the domain name system (DNS) in a far more drastic step towards digital isolationism (Sherman, 2021). Brazil not only passed *Marco Civil da Internet* in 2014 and its general data protection law (known

as “LGPD”) in 2018 but also took concrete steps to construct undersea cable EllaLink connecting Brazil directly to Portugal and by proxy Latin America to Europe to bypass the U.S. surveillance (Yahoo! News, 2022). India started to build a real-time payment system Unified Payments Interface since 2009 (See Hariharan and Natarajan’s chapter in this volume) to foster a thriving national e-payment ecosystem and has drafted or passed several important data legislations. Post-Snowden, South Africa’s digital sovereignty agenda also emphasizes securitization and cyberdefense, although such measures also raise concerns for state surveillance and censorship (See Calandro’s chapter in this volume).

Besides legislative measures focused on data, state digital sovereignty is often expressed in discourses, projects and actions of independence that blend into “postcolonial digital sovereignty” (see below). The colonial legacy in the Global South leads BRICS nations to frequently do so, even though the “state digital sovereignty” perspective is applicable to developed countries too. For example, the Science Council of Canada advocated for “technological sovereignty” as early as 1967 (Globerman, 1978, p.43). After Snowden revelations, Deutsche Telekom proposed a “national internet” to bolster Germany’s digital independence (Deutsche Welle, 2013). As such, the assertion of state digital sovereignty through legislation, research and development projects should not be deemed as negative or positive per se merely because it is branded as “digital sovereignty” and promoted by states. The past two decades demonstrate that both legitimate claims and abusive goals can underpin state assertion of digital sovereignty. Ironically, a global Internet has not rendered the nation state or its sovereignty obsolete. Instead, the pendulum is currently swinging towards de-globalization and re-nationalization of cyberspace.

Supranational Digital Sovereignty

The claim to digital sovereignty, as noted previously, is not limited to the nation-state. Small and mid-sized countries, in particular, face the perennial challenge of navigating power

imbalances (see Doshi & Delgado's chapter in this volume). The European Council on Foreign Relations, for instance, has publicly endorsed a "sovereign Europe" and "digital sovereignty" strategy to enhance its capacity to act (Leonard & Shapiro, 2020). EU has not only embarked on a legislative restructuring of its digital policies to restrict the undue influence and abuse of dominance by U.S. tech giants and in doing so setting global standards, it has also teed digital sovereignty and technological "strategic autonomy" as top priorities (Michel, 2021).

This European desire harkens back to at least 2005 when a few European nations, led by France, proposed the creation of a Euro-centric search engine to compete against Google and Yahoo!. At the time, former French President Jacques Chirac promised to fund Project Quaero to counter the perceived "threat of Anglo-Saxon cultural imperialism" (Litterick, 2005), although after Germany withdrew in 2006, the project fell apart. As the Ukraine war unfolded, EU strengthened its transatlantic ties with the U.S. On the other hand, witnessing the severe economic sanctions U.S. and EU imposed on Russia and the seizing of Russia central bank's overseas assets by the U.S. due to its invasion of Ukraine, not legal by U.S. Treasury Secretary Janet Yellen's own admission (Lawder, 2022), many developing countries may reconsider their economic, political and technological alliances in a U.S. dollar-denominated and –dominated global economy (CGTN, 2022). As the world has moved in a more multipolar direction with the creation of ASEAN in the 1960s, Mercosur in the 1990s, and Africa Continental Free Trade Area in 2019, developing nations are likely to strengthen their digital policy alignment even though they may not achieve the same level of political coordination the EU seems to have maintained so far.

In contrast to EU's more uniform supranational stance of digital sovereignty as well as growing consensus in OECD countries (OECD, 2022) and ASEAN countries (ASEAN, 2012; 2022) in adopting data-related standards, BRICS nations have only taken initial steps to

explore multilateral digital initiatives and cooperation while maintaining their state sovereignty stance. Previously, BRICS summits have issued declarations to address common security challenges in ICT use, promote the global cybersecurity rules within the UN, foster digital development initiatives, and even establish "intra-BRICS" legal frameworks of cooperation. However, concrete multilateral agreements are yet to be hammered out in many areas including tariffs, e-commerce, data protection, cross-border data transfer, technology transfer, cybersecurity, knowledge sharing and so on (Belli, 2021a; Observer Research Foundation, 2021). To what extent BRICS nations will negotiate between their state digital sovereignty and multilateral digital sovereignty in the bloc remains to be seen. However, should BRICS choose to adopt a set of binding digital agreements, the bloc would hold considerable sway in setting global digital standards and in conducting data trade and e-commerce given it represents more than 25% of global GDP and more than 40% of the world's population.

Network Digital Sovereignty

The idea of cyberspace as a separate space exempted from traditional state jurisdiction, or even a sovereign in its own right, is almost as old as the Internet itself. John Perry Barlow's manifesto *A Declaration of the Independence of Cyberspace* (1996) exemplifies this romantic perspective. His proclamation asserts cyberspace's independence *from* nation-states:

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

Bold or naïve, the manifesto taps into the public's yearning for freedom and aversion to state control of the new digital frontier. While Barlow seriously underestimated governments'

persistent power, the utopian sentiment to reject nation states in cyberspace lived on. In the essay *Against Sovereignty in Cyberspace*, Mueller (2019) maintains the importance of network interoperability, de-territorialized cyberspace as a global commons, and non-state governance of the Internet (e.g. ICANN) that prioritizes civil society and the private sector. While grounded in understandable and popular sentiments such individual freedom, mistrust of government and preference for multistakeholderism, a weakness of this approach lies in the very flawed international system of asymmetrical power in which global digital governance is embedded. Realpolitik still favors powerful states and their capacity to enforce laws domestically and extend influence extraterritorially (e.g. GDPR's extraterritorial power and U.S. global dominance through the proxy of its private firms). In retrospect, the Internet has long been treated as a medium to socialize, transact, and mobilize rather than as a by-product of a unique stage of capitalism (Zuboff, 2019) where essentially a handful of global firms—aided by their governments, mostly the U.S. and China—use it to deploy products and services to create profits and accrue power based on endless extraction, surveillance and commodification of user data.

It is worth to note the meaning of "cyberspace sovereignty" or "Internet sovereignty" can vary. Barlow's or Mueller's approach evokes a global commons where "states cannot assert sovereignty over cyberspace" (Mueller, 2019, p.790). The Chinese or Russian use of "Internet sovereignty" notably means exactly the opposite, more akin to the UN-based, state-centric, territorial model (Jiang, 2010) and the "state digital sovereignty" perspective outlined above. In theory, national authorities cannot extend control over users, services, applications or devices outside of their national jurisdiction. In reality, however, state actors such as the NSA or data protection authorities of EU member states acting according to GDPR routinely assert extraterritorial influence. China's latest expansion of its extraterritorial

reach through data laws, mirroring the EU policy, attempts the same (See Cong's chapter in this volume).

Corporate Digital Sovereignty

Exploited by market-centric neoliberalism, the turn from counterculture to cyberculture reimagined Cold War computers as tools for personal liberation, virtual communities as utopian communes, and the digital frontiers as realms of egalitarianism (Turner, 2006). The ascendance of U.S. tech giants since the 1990s and their recent Chinese counterparts birthed a new class of outsized corporate sovereign powers in the digital age. Traditional sovereigns are marked by their authority, legitimacy based on God or law, and supreme power over a territory (Philpott, 2003). These new corporate digital sovereigns (MacKinnon, 2012) have amassed enormous power with little accountability in the digital spaces they create, deriving legitimacy to operate regionally or globally through intellectual property regimes and multilateral trade agreements to wield supreme power over cyberspace.

Tech companies exercise their Corporate Digital Sovereignty through their "structural power" (Strange, 1988) by shaping the functioning of the societies, economies, and democracies through the technologies they provide. Hence, the technological architectures and contractual terms of service they unilaterally define can be seen as the regulatory tools allowing corporate entities to exercise and implement quasi-normative, quasi-executive and quasi-judicial powers that underpin their Corporate Digital Sovereignty (Belli, 2022).

Corporate Digital Sovereignty is the by-product of a new era of capitalism: "surveillance capitalism" (Zuboff, 2019). Unlike industrial capitalism that made commodities out of nature (e.g. real estate), labor (e.g. salary), money (exchange) (Polanyi, 1980/1944) or post-industrial capitalism that commodified things like risk (e.g. insurance) and reputation (e.g. PR), surveillance capitalism is based on the extraction, aggregation and selling of behavioural data and human experiences, often without users' knowledge or against users'

interest (Zuboff, 2019). While corporate digital sovereigns have thrived in a neoliberal environment of free market, privatization, lax regulation and weak industry self-regulation (Radu, 2019), the tides have turned following the crises of the NSA scandal, foreign interference in the 2016 U.S. presidential election, the Facebook-Cambridge Analytica scandal, and Covid-19 misinformation. U.S. tech giants have been targeted by several regulatory probes (albeit with limited efficacy) and Chinese tech titans have also faced increasing charges of neo-colonialism (French, 2015) and enormous pushbacks from the U.S. amidst intense trade wars and geopolitical rivalries between the world's two great powers.

While an increasing number of government initiatives aim at reigning in the excesses of tech giants, especially those based in the U.S., so far such initiatives have been anemic in effecting change despite well-documented negative externalities of such firms in multiple areas including taxation, personal data protection, fair competition, etc. For example, six Silicon Valley giants reportedly created a $100 billion global tax shortfall between 2010 and 2019 by shifting profits from higher-tax jurisdictions to lower-tax or no-tax jurisdictions (Fair Tax, 2019). Despite the recent agreement on a global minimum tax rate of roughly 15% to stop such practices, promoted by the OECD and adopted by the Group of 7 and the Group of 20, taxation of these tech giants has been limited by the agreement (Scott & Birnbaum, 2021).

Personal Digital Sovereignty

The claim to personal digital sovereignty—individual exercise of power and control over personal technologies, data and personhood (Couture & Toupin, 2019)—has deep philosophical roots. Classical philosophies of individualism affirm the intrinsic value of the individual with precedence over the collective or the state in many modern democratic societies (Swart, 1962). Personal digital sovereignty is also associated with a broad set of civil and political liberties such as autonomy and self-determination which in turn have been appropriated by social and political movements on both the left and the right (Robinson et al.,

2017). Moreover, the recent claim to personal digital sovereignty reflects a backlash against the excesses of surveillance capitalism. Bulk collection of individual data, targeted political ads and misinformation-amplifying algorithms have not only eroded individual and public trust in powerful states and tech giants but also exposed the limits of industry self-regulation.

Ultimately, personal data—created, collected, and stored on an unprecedented scale in contemporary digitized societies—is always about someone, deeply connected to personhood (Koopman, 2019). Whether a Lacanian psychoanalytic subject or a Foucauldian political subject, the individual has both intrinsic needs and incentives to avoid the Other's excessive gaze to preserve one's privacy, personhood and control over personal data (Epstein, 2016). This is precisely the rationale behind the formulation of a fundamental right to "informational self-determination" by the German Federal Constitutional Court (1983) in the landmark Census case, arguing this right must be considered as an expression of the right to the free development of personality. In this perspective, every individual has not only a legitimate expectation but a constitutional right to exert control over personal data to know what information about him or her is collected, by whom, for what purposes and with whom it will be shared. As such, any processing of personal data is in principle regarded as an interference with the right to informational self-determination, unless the data subject has consented or the law considers such processing as necessary and proportionate to achieve a legitimate aim.

Similar considerations led the Supreme Court of India to recognize the right to privacy in the landmark Puttaswamy case (Bhandari, Kak, Parsheera & Rahman, 2017) and the Brazilian Supreme Court to enshrine "informational self-determination" as a grounding principle of the Brazilian data protection law (IAPP, 2020). However, the blurry boundaries between our physical and datafied bodies (van der Ploeg, 2012) as well as the surveillance capitalism logics increasingly jeopardize our autonomy and self-determination. In practice, widespread surveillance exposes the enormous distance between the ideal and the reality of

informational self-determination. Rising discourses and practices of personal digital sovereignty now attempt to bridge the gap through the adoption of technologies, including encryption and free or open source software and hardware, as alternatives to mainstream applications and services to minimize state or corporate surveillance, manipulation and decision-making that limit individual choices and agencies.

Users in BRICS countries have been pushing back too, to varying degrees, on both excessive business and state intrusions in their informational self-determination. Whether it is a Chinese university professor suing a local wildlife park over facial recognition data collection without consent (CGTN, 2021) or the retired Indian justice Puttaswamy challenging the constitutionality of the Indian electronic ID system "Aadhaar", individual users in the Global South are increasingly resorting to both legal and non-legal recourses to raise public awareness, change social norms, if not seeking full-scale legislative intervention, to preserve personal digital sovereignty. The demand can also take collective forms as citizens in BRICS countries staged impressive resistance against censorship, surveillance and shutdowns. Indian farmers protested against agriculture laws and severe internet shutdowns (BBC, 2021) before winning concessions from Modi government. Chinese users also successfully pushed back Alibaba affiliate Ant Financial's unauthorized data sharing across Alibaba services and third-parties (Wade, 2018).

Postcolonial Digital Sovereignty

Postcolonial thought and discourse have also informed various claims to digital sovereignty made by both indigenous populations and developing countries with colonial legacies. Previously, scholars have explored Australian indigenous data sovereignty (Kukutai & Taylor, 2016) and first-nation Indian network sovereignty (Duarte, 2017). Core issues of sovereignty involving data and network were raised by such works: Australian indigenous people's jurisdiction over data akin to the indigenous jurisdiction over territory, which would

confer access, possession, control and ownership of indigenous people's own data; the deficiency of American Indian tribes to exercise information and cultural sovereignty due to the lack of network infrastructure and indigenous digital content.

Beyond the calls to restore and enhance indigenous populations' power and control over their own data and networks, postcolonial digital sovereignty discourses also stem from the structural asymmetry and digital divide between developed and developing countries due in no small part to centuries of slavery, predatory practices and unfair international norms. In various digital technology fields, the relationship between America and the rest of the world has often been viewed as one of center-periphery that replicates colonial relations (Garcia, 2022) through Silicon Valley's digital expansions and endless extractions of user data for profits that perpetuates economic and cultural dependencies. ICANN, initially contracted with the U.S. Department of Commerce and eventually separated from it, was unanimously criticized as an instrument of U.S. domination that often favored industrial and Western interests. While a private sector-led domain name system may seem neutral and convenient, it can continue to serve U.S. interest and its global influence as the American private sector operates as de facto proxy to cultivate "the perception of market-based private ordering" (Bruner, 2008).

BRICS nations' claims to postcolonial digital sovereignty harken back to earlier times such as the Non-Aligned Movement in the 1950s, following decolonization and the New World Information and Communication Order (NWICO) movement in the 1970s and 1980s (See Thumfart's chapter in this volume). In the Non-Aligned Movement, countries in Asia, Africa and Latin America tried to abstain from alliance with either America or the U.S.S.R. in support of self-determination against colonialism or imperialism. The NWICO debate led by the MacBride Commission was similarly concerned about economic, culture and media inequality experienced by the Global South as a legacy of colonialism and imperialism

(Fuchs, 2015). This form of international alliance of Postcolonial Digital Sovereignty intersects with other types of anti-colonial efforts by states, individuals and communities. In recent years, whether it's the Brazilian decision to adopt free and open software (adopted in 2003 by the Lula administration and later abandoned by the Temer administration in 2016), Russia's plan to build digital fences to protect the "RuNet", India's rejection of Facebook's zero-rating service Internet.org, China's adoption of a new Data Security Law, or community efforts in South Africa, India or Brazil to create their own community networks, post-colonialism and anti-imperialism continue to find new expressions in current times.

Commons Digital Sovereignty

Beyond the postcolonial perspective, commons digital sovereignty—the idea of building digital public goods for digital commons such as free and open-source software and services or community networks—tries to transcend state and corporate limitations. In this approach, technologies are developed from and for civil society (Haché, 2017), driven largely not by bureaucratic power or profit but by social movements to create alternative forms of digital sovereignty (Couture & Toupin, 2019). The altruistic motivation draws inspirations from the hacker culture in the 1970s and the free and open-source software (FOSS) movement, epitomized by the GNU (2022) project launched by Richard Stallman in 1983. The popular Linux operating system, the success of Wikipedia and growing adoption of Fediverse (Mastodon) for social media are examples of the potential of the FOSS movement (see Tomaz's chapter in this volume).

The increasing development of community networks globally including in several BRICS countries—Brazil, India, and South Africa—highlights the evolving nature of new forms of Commons Digital Sovereignty. As crowd-sourced collaborative digital infrastructure networks, community networks are quintessential expressions of Commons Digital Sovereignty. They are developed in a bottom-up fashion by groups of individuals, *i.e.*

communities which design, manage and maintain the network infrastructure as a common resource. Thus, the communities and the Commons Digital Sovereignty of their members are the core elements of community networks as they are essential to initiate, maintain and guarantee the success of such connectivity efforts (Belli, 2019). In fact, community networks are managed according to the governance models established by their community members in a democratic fashion and can be operated by groups of self-organised individuals or entities such as non-governmental organisations (NGOs), local businesses or public administrations.

Besides providing access to previously disconnected populations, these networks are particularly interesting as they give rise to an ample range of positive externalities to maximise the network self-determination of large groups of individuals (Belli, 2017). These positive external effects include the construction of new infrastructure with limited investment, the engagement of locals in the development of new self-governance models, the revitalisation of social interactions amongst local community members and the emergence of new opportunities for accessing information, learning, and creating employment (Belli, 2019).

It is worth to note that the commons digital sovereignty approach—the collective production of digital public goods—is increasingly seen by small- and mid-sized countries as an important strategy to help ameliorate or overcome the dominance of digital superpowers of the U.S. and China. Not only are countries like France interested in creating new digital commons to avoid the "enclosure" and "exclusivity" of current commercial model (French Ministry of European and Foreign Affairs, 2020), BRICS countries like India also invest in digital public goods to maximize their autonomy against structural dependence on great powers and their tech giants (See Delgado & Doshi's chapter in this volume). For instance, starting from 2003, the Lula administration in Brazil forged an alliance with Free and Open-Source Software (FOSS) activists, adopting open source software as a national policy

as a path to digital sovereignty and digital common good (Kim, 2005). The Indian government has used open-source software and Digital Public Infrastructure in constructing the Indian payment system to leapfrog developed countries (see Hariharan & Natarajan's chapter in this volume).

At the BRICS level, the *New Delhi Declaration* (2021) adopted at the 13th BRICS Summit, endorses a commons digital sovereignty approach. In principle, BRICS promotes the use of "innovative and inclusive solutions, including digital and technological tools to promote sustainable development and facilitate affordable and equitable access to global public goods for all" (BRICS, 2021, section 14). In implementation, BRICS line agencies are encouraged to develop a BRICS Platform on Digital Public Goods as a repository for all open-source technology applications created by BRICS members (BRICS, 2021, section 37). For smaller BRICS countries, the creation and repository of digital public goods contribute to "Sustainable Development Goals" that help BRICS and other developing countries to reap the benefit of global digital commons, all the more urgent during the COVID-19 pandemic in distributing vaccines by the increasingly restrictive commercial intellectual property regimes.

The commons digital sovereignty approach may be particularly relevant in an era of billionaire ownership of public utilities, be it Bezos's ownership of Amazon, Zuckerberg's reign at Facebook, Brin's and Page's ownership of Google and Alphabet, or Musk's take-over of Twitter. Overall, the commons digital sovereignty approach—developed by civil society or nation-states in support of this vision—allows for an alternative way to chart the digital future and its governance that is currently dominated by digital superpowers.

Summary of Contributing Chapters

The book is divided into three segments, bookended by an introductory chapter and a conclusion chapter. The introductory chapter lays the theoretical foundation for the book by disentangling the contesting discourses and interpretations of digital sovereignty informed by

a wide range of literature. The concept of digital sovereignty itself is viewed as a site of power contestation and knowledge production rather than default acceptance. Specifically, seven major perspectives on digital sovereignty are identified from a complex discursive field (see Table 2): state digital sovereignty, supranational digital sovereignty, network digital sovereignty, corporate digital sovereignty, personal digital sovereignty, postcolonial digital sovereignty, and commons digital sovereignty. The chapter outlines who are actively shaping the definition of digital sovereignty and what perspectives and concepts inform the various discourses of digital sovereignty with what purposes. We also highlight affinities and overlaps as well as tensions and contradictions between these perspectives on digital sovereignty with brief illustrative examples from BRICS countries and beyond. While a state-centric perspective on digital sovereignty is traditionally more salient especially in BRICS contexts, increasing public concern over user privacy, state surveillance, corporate abuse, and digital colonialism has given ascendance to a wider array of alternative perspectives on digital sovereignty that emphasize individual autonomy, indigenous rights, community wellbeing and sustainability.

The subsequent eight chapters form the main body of the book, divided into three parts. Part I "State-centric Formations of Digital Sovereignty" recognizes the popular and dominant discourses of digital sovereignty predicated on the nation-state in BRICS countries. This segment includes three chapters: Thumfart's contribution (Chapter 2) that traces the historical imaginaries of digital sovereignty by the Chinese, Russian and Indian governments from NWICO and WSIS to SCO and BRICS; Cong's work (Chapter 3) that outlines the spatial expansion of China's digital sovereignty in its recent national digital legislations; and Calandro's summary (Chapter 4) of the South African approach toward digital sovereignty caught between securitization and development. Part II "Techno-economic Structurings of Digital Sovereignty" focuses on the implementation of digital sovereignty through technical

and financial infrastructures in the BRICS: Hariharan and Natarajan's examination (Chapter 5) of Indian government's open-source digital payment system as an instrument of the country's digital sovereignty; Doshi and Delgado's investigation (Chapter 6) of India and Brazil as examples of "middle powers" with capacity to pursue autonomy and safeguard their digital sovereignty in technical and financial sectors; and Calzati's comparative work (Chapter 7) of Chinese tech giant Huawei's smart city initiatives in South Africa and Italy where corporate digital sovereignty intersects and negotiates with those of the states and local communities. Part III "Grassroots Contestations of Digital Sovereignty" features two chapters: ResisTIC project team's examination (Chapter 8) of the Russian public's resistance to the state-imposed "sovereignization" of the RuNet; and Tomaz's study (Chapter 9) of the Brazilian Internet activists' discourses and practices in Mastodon, a commons-based alternative to commercial social media networks.

More specifically, Thumfart's chapter (Chapter 2) sets the historical context by outlining how China, Russia, and India—three member countries of BRICS and the SCO (Shanghai Cooperation Organization)—constructed imaginaries of "digital sovereignty" since the 1990s. Borrowing the concept of "sociotechnical imaginaries", this chapter examines the regulatory rhetorics, frameworks and policies employed by the three countries from a state-centric perspective of digital sovereignty. He argues these sociotechnical imaginaries are centered on protecting national cultural identity, or "cultural sovereignty", against the "free flow of information", a motive that harkens back to the NWICO debates about the imbalance of media and information flows in the 1970s and 1980s as well as the WSIS discussions surrounding digital and knowledge divides in the information society in the 2000s. In particular, he deduces the development of these three countries' "digital sovereignty" imaginaries from their unique histories, governing approaches and global outlooks, whether it is grounded in the Chinese political philosophy of "tianxia" (under heaven), or the "Russian

world" to restore Russia's traditional influence on the world stage, or India's anti-colonial tradition coupled with its recent drift towards digital authoritarianism. In the transnational evolution of digital sovereignty imaginaries, the SCO seems to have played a role in disseminating regulatory discourses, norms and practices from China to Russia and India. Thumfart concludes if BRICS countries are to construct discourses and practices of digital sovereignty beyond U.S. hegemony, they need to consider both the strengths and weaknesses of their approaches grounded often in state-centric and postcolonial claims to digital sovereignty.

Turning to China, Wanshu Cong's chapter (Chapter 3) explores the Chinese government's legal strategies to counter EU's and US's regulatory reach and extend its digital sovereignty in cyberspace. She argues while China's reterritorialization of its cyberspace is well known, China's emerging tendency to claim extraterritoriality deserves more attention. By closely analyzing recent Chinese legislation—*Personal Information Protection Law, Data Security Law,* and the order by the Ministry of Commerce on blocking unjustified extraterritorial application of foreign legislation and measures, Cong detects a regulatory shift from territoriality to extraterritoriality. A more spatially expansive notion of "digital sovereignty", her chapter argues, is manifested in two approaches: expanding the territorial scope of application of new data governance legislation as well as blocking and countering foreign measures deemed discriminatory or restrictive against China. Emulating EU and US regulatory approaches, these new measures by the Chinese government either directly expand the legislative jurisdiction or produce extraterritorial effects to protect Chinese sovereignty and interest and to counterbalance the extraterritorial reach of foreign regulatory powers. Taken together, these measures reflect the intricate interaction between China's digital sovereignty and current geopolitical circumstances.

Discussing South Africa, the last country placed alphabetically in the BRICS grouping, Enrico Calandro's chapter (Chapter 4) centers on South African digital sovereignty at the crossroad of securitization and ICT development. It explores South Africa's approach to digital sovereignty by analyzing its digital policies and regulations as well as its posture in the context of globalization. The author notes that like many other African countries, South Africa is crafting strategies, policies and rules to frame the increasingly essential role played by ICTs. This process is fraught with tension. On the one hand, South African authorities are struggling to cope with increasing responsibilities of state actors to protect citizens' rights while guaranteeing safety and security online. On the other hand, measures aimed at pursuing public-interest goals, such as data protection and cybersecurity, do not always protect citizens' fundamental rights. Instead, the increasing body of norms, rules and regulations for the digital space risks expanding state control over private communications, facilitating surveillance and online censorship. In terms of digital sovereignty, Calandro analyzes South African's priorities and positions within the global geopolitical governance of cyberspace, highlights the emergence of a securitization agenda in reaction of cyber threats, and interrogates how policy processes and citizens' rights are impacted by the South African position on digital sovereignty.

Turning attention to economic issues, Venkatesh Hariharan and Sarayu Natarajan's chapter (Chapter 5) explores how the Indian state asserts its digital sovereignty by constructing the Unified Payment Interface (UPI) overseen by the National Payment Corporation of India (NPCI), the latter an entity regulated by the Reserve Bank of India. Their case study demonstrates vividly how such indigenous digital payment design, architecture, and governance mechanisms allow for accessible, secure and interoperable transactions in a mobile-first, open API-based payment network to increase financial inclusion. It also illustrates the need to reduce India's dependence on foreign financial

systems, and thus better protected from the shocks that could result from sanctions imposed by foreign states. However, such a system, they argue, is not without potential drawbacks, some of which include the dominance of foreign entities (e.g. Google Pay and PhonePe owned by Walmart/Flipkart) on UPI as well as state-sanctioned monopoly that tends to minimize civil society participation or competition. Besides interoperability and risk mitigation, the authors also advocate a multi-stakeholder governance model for the national digital payment system that bolsters public ownership and institutional checks and balances, a potential model for creating global public digital goods.

Situating their exploration of the digital sovereignty debate in a comparative framework, Vashishtha Doshi and Henrique Delgado's chapter (Chapter 6) considers India and Brazil as examples of "middle powers" and analyses their capacity to pursue autonomy and safeguard their digital sovereignty. The authors seek to answer two broader questions. First, what agency do middle powers master to safeguard their digital sovereignty. Second, to what extent can domestic politics structure the outcome of this available agency. This chapter focuses on the role firms play when great powers weaponize interdependence in finance and digital technology, and subsequently explore the variables along which middle powers can attain autonomy in the above two fields. The authors contend that middle powers have agency to seek autonomy for themselves and reinforce their digital sovereignty. In particular, data localization policies—structuring jurisdiction over data—play a major role in shaping a country's digital statecraft.

In another comparative chapter (Chapter 7), Stefano Calzati considers corporate digital sovereignty's entanglement with national, supranational as well as local communities. His discourse analysis of Chinese tech giant Huawei's corporate approach to digital sovereignty in South Africa and Italy highlights its intersections with national (and supranational) digital sovereignty goals and local communities' desire to achieve autonomy

and control. Two smart city initiatives—Huawei's OpenLab in Johannesburg and Huawei's Joint Innovation Center (JIC) in Italy—are analyzed to show how the posture of the Chinese corporation can vary according to the national context, thus modulating its impact on the construction of corporate digital sovereignty. The comparative case studies not only draw from the role of China in Africa's ICT development but also competing visions of Internet governance informed by "digital sovereignty" and "data colonialism". Taking a critical approach toward "smart cities", Calzati shows while Huawei partners with local private and public actors in Italy, its initiatives in Africa might frustrate South African authorities' hopes of strengthening national digital sovereignty through integrated local tech initiatives. His analysis reveals digital sovereignty is an increasingly entangled transnational geo-governance issue. Whether tech initiatives foster local digital ecosystems and strengthening local digital sovereignty, or end up creating, reproducing or reinforcing power asymmetries depends on specific local, national and international contexts.

In their chapter on *Circumventing the "sovereignization" of the Russian Internet* (Chapter 8), the ResisTIC project team presents the clash between two perspectives on digital sovereignty in the Russian context, namely state digital sovereignty and personal digital sovereignty. The evolution of the Russian government's efforts in implementing the nationalist vision of Internet sovereignty runs against an impressive array of civic tactics of circumvention and evasion. Importantly, the chapter notes that the first decade of the 21st century has been characterized by relatively high levels of freedom in digital innovation in Russia. Since the early 2010s, regulations aimed at establishing Internet sovereignty in Russia have increased as authority of Roskomnadzor, the regulatory body in charge of overseeing media and ICTs, has been substantially expanded. This chapter explores the core elements and limits of Russia's digital sovereignty strategy, which is centered on the "sovereignization" of the RuNet to limit the influence of foreign agents and technology

through the implementation of Internet sovereignty norms and technical tools. Despite Roskomnadzor's tactics of websites blocking and control of online content through a network of technical intermediaries, activists are continuously learning and using new techniques of circumvention. In the digital sovereignty debate, Russian is highly relevant as it is often deemed a "laboratory" of broader authoritarian Internet "sovereignization" tendencies, thus allowing one to observe and conceptualize the changing patterns in digital policies and politics.

Grounded in a commons digital sovereignty perspective, Tales Tomaz's chapter (Chapter 9) documents and critiques the Brazilian FOSS (free and open sources software) movement through a case study of Brazil's participation in Mastodon, a decentralized federated social media platform. This chapter invites readers to consider and imagine alternatives to corporate digital sovereignty, symbolized by the highly centralized and commercialized tech ecosystem concentrated in the hands of a few Silicon Valley monopolies. As the latest iteration of FOSS activism with regard to social media, Mastodon and the larger project of Fediverse present themselves not only as attempts to develop alternative software and tech ecosystems but also as ambitions to build social movements to transform regimes of intellectual property and surveillance capitalism. While the author remains optimistic about a decentralized, community-driven, privacy-enhanced future, the chapter also cautions against potential pitfalls such as the critical mass needed in user adoption, control over digital infrastructure, persistent digital divide between central and peripheral countries as well as power differentiations along racial, class, gender and organizational dimensions.

The final chapter by Belli and Jiang (Chapter 10) acknowledges both the fluidity and the complexity of the notion of digital sovereignty in the BRICS, while also highlighting the necessity of digital sovereignty strategies, policies, and governance mechanisms from a

policymaking 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, or a state. In such contexts, this chapter takes an agnostic approach to digital sovereignty, exploring a selection of practices and providing insight into what this fuzzy theoretical concept means in practical terms. Indeed, digital technologies can facilitate enormous advancements but can also be weaponized against individuals, corporations, and nation states. BRICS countries' approaches offer some telling examples of how and why the need for digital sovereignty can emerge, but also how confused, and even dysfunctional the implementation of policies aimed at digital sovereignty may become. The heterogeneity and cultural richness of the BRICS is also visible in their approaches to digital sovereignty. Importantly, the differences in their approaches are partly explained by their political stances. Russia and China have played a traditionally antagonistic role to the main digital technology power, the U.S., and have more structured approaches to digital sovereignty, given the high risks they associate with the lack of such approaches. The other three members of the grouping have less antagonistic but strong historical reasons for being particularly attached to their (digital) sovereignty. These span from post-colonial sentiments to decades of engagement in the Non-Aligned Movement, to sensitivities raised by recent U.S. abuses of its dominance in digital technologies. Ultimately, BRICS instances illustrate that enhancing a digital sovereign's self-determination, cybersecurity, and control will inevitably reduce the those of other digital sovereigns, likely leading to conflict in the absence of shared and mutually accepted frameworks.

Conclusion

While once imagined as an instrument for a borderless "global village," the Internet is currently undergoing complex processes of re-nationalization (e.g. China, Russia, India) and

regionalization (e.g. EU). BRICS countries, like many others around the world, are grappling with conflicting sets of realities and desires: individual privacy and national security, data localization and cross-border data flows, digital independence and international technological trade, often driven by concurrent national priorities, international commitments, and ambitions for global expansion and influence.

This book volume focuses on the central idea of "digital sovereignty" in digital policymaking, disentangles the myriad discourse and interpretations of digital sovereignty, and views the idea itself as a site of power struggle and knowledge production. Toward this end, we mapped out seven theoretical perspectives on "digital sovereignty": beyond the traditional perspective of state digital sovereignty, we also included supranational digital sovereignty, network digital sovereignty, corporate digital sovereignty, personal digital sovereignty, postcolonial digital sovereignty, and commons digital sovereignty. While the seven perspectives may not be entirely mutually exclusive, they offer analytical lenses to examine the different discourses and approaches towards "digital sovereignty". The book's concluding chapter will offer more practical examples of and reflections on BRICS countries' digital sovereignty experiences to bookend the effort.

Collectively, we are fundamentally interested in who is actively shaping the definition of digital sovereignty, what perspectives and concepts inform the myriad interpretations of digital sovereignty with what purposes, and how they are applied in a wide range of areas in BRICS countries with what potential impact and challenges ahead. Not only does this collective effort draw on the experiences, practices and reflections of digital sovereignty from the BRICS scholarly community that contributes to the global conversation on the subject, it also offers a forward-looking take on what a digital world less dependent on a handful of Silicon Valley or Chinese tech giants might look like in a post-Snowden, post-Facebook-Cambridge Analytica, and post-digital superpower world. Given BRICS

countries' growing international relevance, we hope the perspectives and issues identified in the book project to be of great importance to the future shape of the global digital world.

References

Allison, G. (2017). Destined for war: Can America and China escape Thucydides's Trap? New York: Houghton Mifflin Harcourt.

Armijo, L. & Roberts, C. (2014). The emerging powers and global governance Why the BRICS matter. R. Looney (ed.), *Handbook of emerging economies* (pp.503-524). New York: Routledge.

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

ASEAN. (2012). *ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN): Framework on personal data protection*. ASEAN. Retrieved from https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

ASEAN. (2022). *ASEAN data management framework: Data governance and protection throughout the data lifecycle*. ASEAN. Retrieved from https://is.gd/DWPKAc

Avila Pinto, R. (2018). Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. *SUR: International Journal on Human Rights, 15*(27), 15-27.

Bai, C. & Lei, X. (2020). New trends in population aging and challenges for China's sustainable development. *China Economic Journal, 13*(1), 3-23.

Barlow, J. P. (1996). *Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. Retrieved from https://www.eff.org/cyberspaceindependence

BBC. (November 22, 2019). *Chaayos cafe: Indian cafe's facial recognition use sparks anger*. BBC. Retrieved from https://www.bbc.com/news/world-asia-india-50499380

BBC. (December 26, 2020). *Chinese economy to overtake US 'by 2028' due to Covid*. BBC. Retrieved from https://www.bbc.com/news/world-asia-china-55454146

BBC. (January 30, 2021). *India protests: Internet cut to hunger-striking farmers in Delhi*. BBC. Retrieved from https://www.bbc.com/news/world-asia-india-55872480

Belli, L. (2017). 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. (2019). Community networks: Empowering individuals, expanding connectivity, promoting network self-determination. In Luca Belli (Ed.), *Building community network policies: A collaborative governance towards enabling frameworks* (pp.13-20). Rio de Janeiro, Brazil: FGV Direito Rio. Retrieved from https://is.gd/33Qjlp

Belli L. (2021a). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. In *African Journal of Information and Communication*, *28*, 1-14.

Belli, L. (2021b). *BRICS countries to build digital sovereignty*. In: Belli, L. (Ed.) *CyberBRICS: Cybersecurity regulations in BRICS countries* (pp.271-280). Berlin, Germany: Springer. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-56405-6_7

Belli, L. (2022). Structural power as a critical element of digital platforms' private sovereignty. In Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (Eds.), *Constitutionalising social media* (pp.81-100). Oxford, UK: Hart Publishing.

Bennett, L. W. & Sederberg, A. (2013). *The logic of connective action: Digital media and the personalization of contentious politics.* Cambridge: Cambridge University Press.

Bhandari, V., Kak, A., Parsheera, S., Rahman, F. (2017). An analysis of Puttaswamy: The Supreme Court's privacy verdict. *IndraStra Global*, *11,* 1-5.

Bond, S. (February 28, 2022). *Facebook and Tiktok block Russian state media in Europe.* NPR. Retrieved from https://is.gd/824rTz

Brazilian Ministry of Foreign Relations. (May 19, 2022). BRICS Joint Statement on "Strengthen BRICS Solidarity and Cooperation, Respond to New Features and Challenges in International Situation" (PRESS RELEASE N. 76). Brazilian Ministry of Foreign Relations. Retrieved from https://is.gd/JU3ioQ

BRICS. (2021). *XIII BRICS Summit-New Delhi Declaration*. BRICS. Retrieved from https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-51.pdf

Broeders, D. & van den Berg, B. (2020). *Governing cyberspace: Behavior, power, and diplomacy*. London: Rowman & Littlefield.

Bruner, C. M. (2008). States, markets, and gatekeepers: Public-private regulatory regimes in an era of economic globalization. *Michigan Journal of International Law, 30,* 125-176.

CGTN. (May 20, 2022). *Rediscover the value of BRICS under 'three pillars'*. CGTN America. Retrieved from https://is.gd/c4pqLy

CGTN. (May 21, 2022). *The heat: BRICS meeting*. CGTN America. Retrieved from https://america.cgtn.com/2022/05/21/the-heat-brics-meeting

Chadwick, A. (2006). *Internet Politics: States, Citizens, and New Communication Technologies*. Oxford, UK: Oxford University Press.

Chander, A. (2020). Is data localization a solution for Schrems II? *Journal of International Economic Law*, *23*(3), 771–784.

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

Couldry, N. & Mejias, U. (2019). *The costs of connection: How data Is colonizing human life and appropriating it for capitalism*. Stanford, CA: Stanford University Press.

Coulthard, S.G. (2014). *Red skin, white masks: Rejecting the colonial politics of recognition*. Minneapolis, MN: University of Minnesota Press.

Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In D. Broeders & B. van den Berg (Eds.), *Governing cyberspace: Behavior, power, and diplomacy* (pp. 107-142). London: Rowman & Littlefield.

Dados, N. & Connell, R. (2012). The global south. *Contexts, 11*(1), 12-13.

Daucé, F. & Musiani, F. (2021). Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction. *First Monday, 26*(5). Retrieved from: https://firstmonday.org/ojs/index.php/fm/article/view/11685/10122

Deutsche Welle (October 21, 2013). *Deutsche Telekom plans for a 'national internet.'* Deutsche Welle. Retrieved from http://is.gd/yLGeyF

Duarte, M. (2017). *Network sovereignty: Building the Internet across Indian country*. Seattle, WA: University of Washington Press.

Economic Times. (July 9, 2015). Not here to compete with IMF, World Bank: NDB chief KV Kamath. Retrieved from: https://tinyurl.com/4hkfx6m7

Economist, The. (May 6, 2017). The world's most valuable resource is no longer oil, but data. *The Economist.* Retrieved from https://is.gd/PQ6Vrj

Epstein, C. (2016). Surveillance, privacy and the making of the modern subject: Habeas what kind of corpus? *Surveillance and Embodiment, 22*(2), 28-57.

EU. (May 31, 2021). *The EU and LAC come together: a 6.000 km high-capacity submarine cable bridges the digital gap between the two continents*. The European Union. Retrieved from https://is.gd/rvyqBu

Fair Tax. (December 2, 2019). *Tax gap of Silicon Six over $100 billion so far this decade*. Retrieved from https://fairtaxmark.net/tax-gap-of-silicon-six-over-100-billion-so-far-this-decade/

Fang, B. X. (2018). *Cyberspace sovereignty: Reflections on building a community of common future in cyberspace*. Singapore: Springer.

French, H. (2015). *China's second continent: How a million migrants are building a new empire in Africa*. New York, NY: Vintage Books.

French Ministry of European and Foreign Affairs. (July 31, 2020). *Barbed wire on the Internet prairie: against new enclosures, digital commons as drivers of sovereignty*. French Ministry of European and Foreign Affairs. Retrieved from https://is.gd/O1RRxy

Fuchs, C. (2015). The MacBride Report in the Twenty-First-Century capitalism, the age of social media, and the BRICS countries. *Javnost*, *22*(3), 226-239.

Garcia, E. V. (2022). The technological leap of AI and the Global South: Deepening asymmetries and the future of international security. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4304540

German Federal Constitutional Court (1983). Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES]. Retrieved from https://is.gd/entUqg

Globerman, S. (1978). Canadian science policy and technological sovereignty. *Canadian Public Policy/Analyse De Politiques, 4*(1), 34–45.

GNU. (2022). *About the GNU Operating System*. GNU. Retrieved from https://is.gd/yQWoEB

Goldsmith, J. & Wu, T. (2006). *Who controls the Internet?: Illusions of a borderless world*. New York, NY: Oxford University Press.

Grimm, D. (2015). *Sovereignty: The origin and future of a political and legal concept* (B. Cooper, Trans.). New York: Columbia University Press.

Haché, A. (2017). *Technological sovereignty Vol. 2*. Barcelona, Spain: Descontrol. Retrieved from https://is.gd/Ntk8b0

Haider, S. & Krishnan, A. (April 17, 2022). BRICS meet likely in June, India to attend China-hosted event. *The Hindu.* Retrieved from https://is.gd/fQQL4p

Havercroft, J. (2011). *The captive of sovereignty*. Cambridge, MA: Cambridge University Press.

Herlo, B., Irrgang, D., Joost, G., & Unteidig, A. (Eds.). *Practicing sovereignty: Digital involvement in times of crisis*. Bielefeld, Germany: transcript Verlag.

Hinck, R., Cooley, S. & Kluver, R. (2019). *Global media and strategic narratives of contested democracy: Chinese, Russian, and Arabic media narratives of the US presidential election*. New York, NY: Routledge.

International Association of Privacy Professionals (IAPP). (2020). Brazilian General Data Protection Law (LGPD, English translation). Retrieved from https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

Indian Ministry of External Affairs. (July 9, 2015). *7th BRICS Summit - Ufa Declaration*. Government of India. Retrieved from https://is.gd/GBKi1M

Indian Ministry of External Affairs. (September 9, 2021). *XIII BRICS Summit- New Delhi Declaration*. Government of India. Retrieved from https://is.gd/ib4Ocy

Jiang, M. (2014). The business and politics of search engines: A comparative study of Baidu and Google's search results of Internet events from China. *New Media & Society, 16*(2), 212-233.

Jiang, M. (2010). Authoritarian informationalism: China's approach to Internet sovereignty. *SAIS Review of International Affairs, 30*(2), 71-89.

Jiang, M. (2020). Cybersecurity policies in China. In Belli, L. (Ed.) *CyberBRICS: Cybersecurity regulations in BRICS countries* (pp.195-212). Berlin, Germany: Springer.

Jiang, M. & Fu, K.W. (2018). Chinese social media and big data: Big data, big brother, big profit? *Policy & Internet, 10*(4), 372-392. DOI: 10.1002/poi3.187

Kim, E. (2005). F/OSS adoption in Brazil: The growth of a national strategy. In Karaganis, J. and Latham, R. (Eds.). *The politics of open source adoption*. New York: Social Science Research Council.

Kovacs, A. & Ranganathan, N. (2019). *Data sovereignty, of whom? Limits and sustainability of sovereignty frameworks for data in India*. Data Governance Network. Retrieved from https://datagovernance.org/files/research/IDP_-_Data_sovereignty_-_Paper_3.pdf

Koopman, C. (2019). *How we became our data: A genealogy of the informational person*. Chicago: University of Chicago Press.

Krasner, S. (1999). *Sovereignty: Organized hypocrisy*. New Haven, NJ: Princeton University Press.

Kuehn, K. M. (2018). Surveillance and South Africa. Book Review: Jane Duncan (2018), Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa, Wits University Press. *The Political Economy of Communication, 6*(2), 94–100.

Kukutai, T. & Taylor, J. (2016). *Indigenous data sovereignty: Toward an agenda (CAEPR)*. Canberra, Australia: ANU Press.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology, 33*, 369-378.

Lawder, D. (2022). *Yellen: Not legal for U.S. to seize Russian official assets*. Reuters. Retrieved from https://is.gd/9qHaGX

Leonard, M. & Shapiro, J. (2020). *Sovereign Europe, dangerous world: Five agendas to protect Europe's capacity to act*. European Council on Foreign Relations. Retrieved from https://is.gd/Cwwos8

Lessig, L. (1999). *Code: And other laws of cyberspace*. New York, NY: Basic Books.

Litterick, D. (August 31, 2005). Chirac Backs Eurocentric Search Engine. *The Telegraph*. Retrieved from http://is.gd/ se2dRa

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for internet freedom.* New York, NY: Basic Books.

Miao, W., Jiang, M. & Pang, Y. (2021). Historicizing Internet regulation in China: A meta-analysis of Chinese Internet policies (1994-2017). *International Journal of Communication, 15*, 2003–2026.

Michel, C. (February 3, 2021). *Digital sovereignty is central to European strategic autonomy - Speech by President Charles Michel at "Masters of digital 2021" online event*. European Council. Retrieved from https://is.gd/mm4ysK

Mueller, M. (2020). Against sovereignty in cyberspace. *International Studies Review, 22*(4), 779–801.

Mukerjee, S. (2016). Net neutrality, Facebook, and India's battle to #SaveTheInternet. *Communication & The Public,* 1(3), 356-361.

National Law Review. (January 6, 2022). *India's draft Data Protection Bill moves closer to passage*. National Law Review. Retrieved from https://is.gd/n3i2kH

New Development Bank (NDB). (2022). *NDB'S member countries*. New Development Bank. Retrieved from https://www.ndb.int/about-us/organisation/members/

Nocetii, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs, 91*(1), 111-130.

Observer Research Foundation (ORF). (August 1, 2021). Digital BRICS: A new framework for cooperation on technology and innovation. Retrieved from https://is.gd/USfmdV

OECD. (2022). *Personal data protection at the OECD*. OECD. Retrieved from https://www.oecd.org/general/data-protection.htm

O'Neill, J. (2001). *Building better global economic BRICs*. Goldman Sachs. Retrieved from https://www.goldmansachs.com/insights/archive/building-better.html

PBS. (September 24, 2013). *Brazilian President condemns NSA spying*. PBS. Retrieved from: https://www.pbs.org/newshour/nation/brazilian-president-condemns-nsa-spying

Philpott, D. (2003). *Sovereignty*. Stanford Encyclopedia of Philosophy Archive. Retrieved from: https://plato.stanford.edu/archives/sum2016/entries/sovereignty/

Polanyi, K. (1980/1944). *The great transformation.* New York, NY: Beacon Publisher Group.

Polatin-Reuben, D. & Wright, J. (2014). *An Internet with BRICS characteristics: Data sovereignty and the Balkanisation of the Internet*. Paper presented at Foci'14. San Diego, CA. Usenix. Retrieved from https://is.gd/pw2ohk

Prashad, V. (2012). *Poorer nations: A possible history of the Global South*. London: Verso.

Radu, R. (2019). *Negotiating internet governance*. Oxford, UK: Oxford University Press.

Reuters. (February 15, 2022). India adds 54 more Chinese apps to ban list; Sea says it complies with laws. *Reuters.* Retrieved from https://is.gd/nlXQCU

Reviglio, U. & Agosti, C. (2020). Thinking outside the black-box: The case for "algorithmic sovereignty" in social media. *Social Media + Society, 6*(2), 1-12.

Robinson, E. et al. (2017). Telling stories about post-war Britain: Popular individualism and the "crisis" of the 1970s. *Twentieth Century British History, 28*(2), 268–304.

Roio, D. (2018). *Algorithmic sovereignty.* [Doctoral dissertation, University of Plymouth]. Retrieved from https://pearl.plymouth.ac.uk/handle/10026.1/11101

Scott M., & Birnbaum, E. (June 30, 2021). How Washington and Big Tech won the global tax fight. *Politico*. Retrieved from https://www.politico.eu/article/washington-big-tech-tax-talks-oecd/

Sheehan, M. & Du, S. (December 9, 2022). *What China's algorithm registry reveals about AI governance*. Carnegie Endowment. Retrieved from

https://carnegieendowment.org/2022/12/09/what-china-s-algorithm-registry-reveals-about-ai-governance-pub-88606

Sherman, J. (2021). *Reassessing RuNet: Russian Internet isolation and implications for Russian cyber behavior*. Atlantic Council. Retrieved from https://is.gd/rcJ0bJ

South Commission. (1990). *The challenge to the South: The report of the South Commission*. Oxford, UK: Oxford University Press.

Sparks, C. (2014). Deconstructing the BRICS. *International Journal of Communication, 8,* 392-418.

Stuenkel, O. (2016). *Post-Western world: How emerging powers are remaking global order*. London, UK: Polity.

Stuenkel, O. (2020). *The BRICS and the future of global order* (2nd ed.). London, UK: Lexington Books.

Swart, K. (1962). "Individualism" in the mid-nineteenth century (1826-1860). *Journal of the History of Ideas, 23*(1), 77-90.

Tan, H. (2023). Russia says its economy did better than expected, one year into the Ukraine war. But experts say there's a red flag behind the announcement. *Business Insider.* Retrieved from https://www.businessinsider.com/russia-ukraine-war-economy-contraction-sanctions-energy-putin-2023-2

Turner, F. (2006). *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, IL: University of Chicago Press.

USCC (U.S.-China Economic and Security Review Commission) (2022). K*ey events and statements summarizing China's position on Russia's invasion of Ukraine*. USCC. Retrieved from https://is.gd/lQ8FUL

van der Ploeg, I. (2012). The body as data in the age of information. Kirstie Ball, Kevin Haggerty and David Lyon (eds*.), Routledge Handbook of Surveillance Studies* (pp.176-183). New York: Routledge.

Wade, S. (2018). *Privacy concerns focus on tech firms, not government*. China Digital Times. Retrieved from https://is.gd/CeKiLc

World Bank. (2020). GDP. Retrieved from https://data.worldbank.org/indicator/Ny.Gdp.Mktp.Cd

Wu, L. (April 21, 2021). *China's first lawsuit on facial recognition made verdict*. CGTN. Retrieved from https://is.gd/UJ94Mp Xinhua Net. (2015). 学习有方：5个词读懂习近平的网络安全新主张 [Study strategies: 5 keywords to understand President Xi's new proposal on cyber security]. Xinhua Net. Retrieved from http://www.xinhuanet.com//politics/2015-08/06/c_128099493.htm

Yahoo! News. (March 9, 2022). *Now interconnecting Brazil and Southern Europe: EllaLink and DE-CIX announce strategic partnership*. Yahoo! News. Retrieved from https://finance.yahoo.com/news/now-interconnecting-brazil-southern-europe-151600489.html

Zittrain, J. (2003). Internet points of control. *Boston College Law Review*, *44*, 653-688.

Zondi, S. (2022). *The political economy of intra-BRICS cooperation: Challenges and prospects*. Palgrave Macmillan.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Washington, DC: PublicAffairs.