Preface

With 40% of the world's population, 25% of global GDP, and large sums of one of the world's most valuable resources – personal data – BRICS countries (Brazil, Russia, India, China, and South Africa) are playing an increasingly important role in global digital development and policymaking. Yet, their conceptions, narratives, and initiatives of digital sovereignty remain surprisingly understudied. This is the first book-length project to explore the digital sovereignty debate from a Global South perspective by analyzing BRICS countries' approaches to digital governance as well as offering a forward-looking take on what a digital world less dependent on a handful of Silicon Valley tech giants might look like and what alternatives there might be.

Just as the BRICS alliance is a developing world's response to the 2008 global financial crisis and the 2009 Euro crisis, triggered by the subprime mortgage crisis in the US, many of the BRICS digital sovereignty initiatives are also expressions of a strong desire to build a multipolar world, seeking independence from and alternatives to a US-centric model of digital development and governance. This book assembles a collection of fine academic analyses of key digital sovereignty issues in the BRICS countries from diverse and complementary perspectives: from historical imaginaries to up-to-date conceptualizations of digital sovereignty, from e-payment systems to smart cities, and from legal analyses to geopolitical assessments. Given the growing international relevance of the BRICS grouping, corroborated by its recent expansion, we expect the perspectives and issues identified in the book will be of great importance to the future debate and shape of global digital governance.

This book makes significant epistemological, theoretical, and strategic contributions to the growing research on digital sovereignty. *Epistemologically*, this is the first book-length project to explore the digital sovereignty debate from an underappreciated Global South perspective, drawing from

https://doi.org/10.1017/9781009531085.001 Published online by Cambridge University Press

discourses and practices in the BRICS countries. This collective effort situates the debate at a critical historical and geopolitical juncture, against the backdrop of the 2013 Snowden Affair, the Facebook–Cambridge Analytica scandal during the 2016 US presidential election, and the recent Russian invasion of Ukraine started in the middle of a global pandemic and economic recession.

The emergence of the BRICS not only represents the "rise of the rest" (Amsden, 2001) in an increasingly multipolar, *post-Western* world (Stuenkel, 2016), it also signifies a *post-global* moment when the world's subalterns recognize the US-led neoliberal globalization experiment as a failed master narrative (Lopez, 2007) in need of a substantial reboot. The ways in which such a reboot may occur, however, are far from clear and deserve great attention. In the digital realm, while once imagined as an instrument for a borderless "global village," the internet is currently undergoing complex processes of renationalization (e.g., China, Russia, and to some extent India) and regionalization (e.g., the 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 self-determination and international technological trade – often driven by concurrent national priorities, international commitments, and ambitions for global expansion and influence.

Theoretically, the book also makes several important contributions to an emerging and prominent debate on digital sovereignty. Importantly, we depart from a normative, legal approach toward (digital) sovereignty centered around the nation-state. Instead, we define "digital sovereignty" as ultimately the exercise of agency, power, and control over digital infrastructure, data, services, and protocols. While Westphalian norms that undergird many of the modern nation-states such as territorial integrity, legal equality, and noninterference still dominate in academic, policy, and public debates about (digital) sovereignty, we recognize that, in reality, borders are repeatedly transgressed, international norms are frequently violated in a world of asymmetrical power, so much so that some argue sovereignty is an "organized hypocrisy" (Krasner, 1999). The gap between norms and reality is especially pronounced in the digital realm where much of the world's digital infrastructure, data, and services remain overly dependent on a handful of Silicon Valley companies that deploy a remarkable level of corporate digital sovereignty (Belli, 2022).

Further, beyond the conventional state-centric interpretation, recent literature on digital sovereignty (e.g., Belli, 2021a; Belli & Hadzic, 2023; Couture & Toupin, 2019; Pohle & Thiel, 2020) has moved to incorporate diverse discursive and policy practices. Increasing public concern over data privacy, state surveillance, corporate abuse, and digital colonialism (e.g., Couture & Toupin, 2019; Zuboff, 2019a) has given ascendance to a wide array of alternative perspectives on digital sovereignty that emphasize individual autonomy, indigenous rights, community well-being, and sustainability. Couture and Toupin's

article (2019), for instance, features *five* perspectives on digital sovereignty: "cyberspace sovereignty," "digital sovereignty, governments and states," "indigenous digital sovereignty," "social movements and digital sovereignty," and "personal digital sovereignty." Our conceptual framework builds on this line of work but extends it to include *seven* theoretical perspectives that can guide contextualized analyses: state digital sovereignty, supranational digital sovereignty, network digital sovereignty, corporate digital sovereignty, personal digital sovereignty, postcolonial digital sovereignty, and commons digital sovereignty. We also demonstrated how these seven perspectives may prove to be particularly useful to inform debates in a single application area such as "data sovereignty" or "algorithmic sovereignty."

Rather than making nation-states the default actors with the legitimacy or capacity to exercise digital agency, power, and control over citizens' data and digital lives, our new theoretical framework recognizes and shows with empirical evidence that a plethora of actors including empowered individuals, companies, communities, and even supranational alliances can pursue and influence digital sovereignty. 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. Questionable business players can also drive multistakeholder efforts in the name of human rights and democracy while stripping away human protection and dignity. Only by asking who can (legitimately) wield agency, 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."

Strategically, this volume acknowledges that BRICS countries' approaches offer some telling examples of not only how and why digital sovereignty may be needed and constructed but also how dysfunctional the implementation of digital sovereignty policies may become without a coherent long-term vision. BRICS countries' experiences underscore the importance of self-determination, strategic autonomy, rights-based frameworks, and governance, whether the "sovereign" is an individual, a community, a corporation, a state, or a group of states. BRICS countries have realized that without sufficient understanding, the development or control of digital infrastructures, data, and services, aspiring "digital sovereigns" are doomed to remain "digital subjects." In this perspective, they have developed technologies, implemented national policies, and made intra-BRICS arrangements to escape technological dependency and try to preserve or construct their capacity to be exert agency, power, and control online. Their digital policies, increasingly influential beyond their national borders, are often considered models in the Global South, even if they are not openly acknowledged as such by policymakers in developed countries.

Importantly, we also need to take BRICS digital sovereignty narratives, policies, and practices with a grain of salt. Indeed, digital sovereignty may be driven by a wide spectrum of motivations, including authoritarian control and protectionism, alongside self-determination and empowerment, which may produce both negative and positive outcomes. On the one hand, such policies may strongly enhance cybersecurity, fiscal justice, and innovation. China, for instance, built the only digital ecosystem that can compete with Silicon Valley over the past three decades. Brazil pioneered the national adoption of open-source software in 2003 to avoid technological dependence. Also, in partnership with the EU, Brazil constructed EllaLink, an undersea cable to connect Brazil directly to Portugal, to circumvent US surveillance and enhance its digital sovereignty. Indian activists staged the impressive #SaveTheInternet movement in 2016 to reject Facebook's dubious Internet.org initiative supposedly to offer more digital freedom to Indians in poverty. Thanks to the prohibition of zero-rating practices, India has become the only Global South country to experience meaningful connectivity, unleashing a new era of innovation and construction of easily accessible digital public infrastructure (DPI). South Africa has developed its own data protection and cybersecurity model, but pernicious practices of censorship and surveillance have also been introduced under the auspice of digital sovereignty that seriously curtail citizens' rights, privacy, and security. Under President Putin, Russia passed the Sovereign Internet Law in 2019 and pursued an intensive process of sovereignization of the Russian segment of the internet, the "RuNet" despite grassroots resistance. BRICS experiences show it is critical to examine not only the discursive claims to digital sovereignty but also the specific actions and outcomes in contexts.

Last but not the least, we are also witnessing a new generation of techno-regulatory initiatives that aim at embedding digital sovereignty into technology to purposefully shape the evolution of society and economy through digital infrastructure. This new approach to policy and regulation by technology, particularly evident in numerous BRICS experiences, deserves academic, policy, and public attention. While not necessarily a trend toward techno-authoritarianism where technology becomes an instrument of control, embedding digital sovereignty into technology can also be a positive exercise of self-determination, allowing individuals, communities, and countries to become the protagonists of their own digital development. The India Stack, for instance, fosters the digitalization of the entire country through the development of DPI based on open-source technology. While not exempt from criticism, it is a fascinating example of digital sovereignty fostered by the state but implemented in a decentralized way by technologists through technology, no less effective than state policy. Similarly, Brazil has embraced DPI by creating Pix, the national electronic payment system established by the Brazilian Central Bank, that in less than three years has become omnipresent, breaking the previous online payment (and ecommerce data) duopoly of Visa and Mastercard

(Belli, 2023). This and other initiatives from BRICS and the Global South need to be carefully studied and understood by researchers, policymakers, and civil society advocates alike, as they hold promise to create entire new avenues for governance, policy, and regulation.

Taken altogether, this edited book volume will contribute to not only epistemological and theoretical debates on digital sovereignty but also their varied applications and perspectives from the Global South and emerging power alliances, critical to the shaping of the world's digital future and policymaking. As such, this book promises to enrich the ongoing and far from settled debate on digital sovereignty and digital governance among scholars, researchers, policymakers, civil society, and businesses in both developed and developing countries.