On the Way to BRICS+ Digital Sovereignty: Opportunities and Challenges of a New Era

Elizaveta Gromova,

National Research South Ural State University (Chelyabinsk, Russian Federation)

Daniel Brantes Ferreira,

Kazan Innovative University named after V.G. Timiryasov (Kazan, Russian Federation)

https://doi.org/10.21684/2412-2343-2024-11-3-54-69

Abstract. A new era for BRICS has begun with the desire of new countries to join BRICS. This expansion, the BRICS+, poses several challenges and opportunities for the renewed alliance, particularly concerning the digital sovereignty of the countries. On the one hand, the leading five BRICS nations have the potential to achieve digital sovereignty, earning the moniker "the hawks of digital sovereignty." On the other hand, expanding BRICS membership to countries with varying levels of digitalization raises issues for the alliance. These include improving national legislation on digital sovereignty and defining actions to foster cooperation within BRICS+. This article aims to design a theoretical legal model for BRICS+ digital sovereignty, outlining its pillars and offering recommendations for achieving digital sovereignty within BRICS+. The comparative legal method, used to analyze regulations in digitalization and digital sovereignty among BRICS+ member countries, ensures a comprehensive understanding of the legal landscape. Retrospective analysis, which studied the development of BRICS+ regulations in these areas, provides a historical context. The systematic method, which examined legal tools and instruments that contribute to achieving digital sovereignty, ensures a thorough exploration. The content analysis allowed for the interpretation of news articles and social media sources related to BRICS+ digital sovereignty, adds a contemporary perspective. The authors conclude that achieving digital sovereignty for BRICS+ is possible and offer several recommendations for collaboration, including developing a BRICS+ digital sovereignty memorandum, launching a BRICS+ regulatory sandbox, and

deploying a BRICS+ sovereign cloud. These recommendations can inform BRICS+ policy-making, contribute to the limited literature in this field, and serve as a basis for future research on BRICS+ digital sovereignty.

Keywords: digital sovereignty; data; digital technologies; security; cyberspace; BRICS; regulation.

Recommended citation: Elizaveta Gromova & Daniel Brantes Ferreira, *On the Way to BRICS+ Digital Sovereignty: Opportunities and Challenges of a New Era*, 11(3) BRICS Law Journal 54–69 (2024).

Table of Contents

Introduction

One of the most important goals of modern states is to create a resilient digital environment and implement competitive national innovations and technologies. This ambitious objective has been set by the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China, and the Republic of South Africa.[1] The BRICS nations are renowned globally as the fastest-growing significant countries.[2] Experts predict that by 2050, the combined economies of the BRICS countries will surpass those of the G-7 nations.[3]

Brazil, Russia, India, China, and South Africa have worked to establish joint positions on crucial social, economic, and political issues through consensus over the years. A new era for BRICS began when Saudi Arabia, Egypt, the United Arab

---

1 Adriana B. Deorsola et al., *Intellectual Property and Trademark Legal Framework in BRICS Countries: A Comparative Study*, 49 World Patent Inf. 1 (2017).

2 *See* Mizuho Research Institute Ltd., Commission of the Economic and Social Research Institute, *Comparative Analysis of the BRICS* (June 2018) (Jul. 1, 2024), available at http://www.esri.go.jp/jp/prj/hou/hou016/hou16a-2-1.pdf.

3 *Коротков С.А., Кульков И.В.* Развитие БРИКС // Вестник ЮНИДО в России. 2013. № 11. С. 54 [Sergei A. Korotkov & Igor V. Kulkov, *Development of BRICS*, 11 Bulletin of UNIDO in Russia 54 (2013)].

Emirates, Ethiopia, and Iran joined as the new permanent members, giving birth to the BRICS+.

To further intensively develop BRICS+ and enhance their potential to hold a leading position among other countries, member countries should stimulate the creation of digital technologies within their borders and establish a collaborative legal framework to ensure digital sovereignty both at the national level and within the union.

The emergence of digital technologies globally has been greeted with immense possibilities for application and significant potential. However, these technologies also pose a threat to national security. Consequently, the concept of digital sovereignty is developing rapidly, and many countries, including BRICS+, have already implemented this concept into their national legislation.

Scholars refer to BRICS countries as "the hawks of sovereignty" due to their efforts to "shape digital space governance based on their respect for sovereignty and non-interference in domestic affairs in the digital space."[4]

An analysis of the literature on digital sovereignty in BRICS+ reveals a limited number of articles and books devoted to this issue. With ongoing discussions about its legitimacy, the term "digital sovereignty" remains debated among scholars.[5] Proponents of digital sovereignty research focus on its definition, key features, and methods for achieving it.[6] Some papers analyze digital sovereignty within one or several jurisdictions.[7]

A chapter related to BRICS digital sovereignty was recently published.[8] The authors analyze the complex and multifaceted concept of BRICS digital sovereignty.

However, the number of scientific works related to BRICS+'s digital sovereignty is limited, with essentially only one article on the topic. Ignatov and Zinovieva have

---

4 BRICS Agenda for Digital Sovereignty, Russian International Affairs Council, 29 January 2024 (Jul. 1, 2024), available at https://russiancouncil.ru/en/analytics-and-comments/analytics/brics-agenda-for-digital-sovereignty/.

5 Margarita Robles-Carrillo, *Sovereignty vs. Digital Sovereignty*, 1(3) J. Dig. Tech. & L. 673 (2023); Milton Mueller, *Against Sovereignty in Cyberspace*, 22(4) Int'l Stud. Rev. 779 (2020); Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 Air Force L. Rev.; Maxwell AFB 1 (2009) (Jul. 1, 2024), also available at https://www.proquest.com/docview/195182873; Kevin J. Heller, *In Defense of Pure Sovereignty in Cyberspace*, 97 Int'l L. Stud. 1432 (2021); Huw Roberts et al., *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, 10(3) Internet Pol'y Rev. (2021).

6 Anupam Chander & Haochen Sun, *Sovereignty 2.0* (2021); Deborah Elms, *Digital Sovereignty: Protectionism or Autonomy* (2021).

7 Stanislav Budnitsky & Lianrui Jia, *Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance*, 21(5) Eur. J. Cult. Stud. 594 (2018); Francesco Crespi et al., *European Technological Sovereignty: An Emerging Framework for Policy Strategy*, 56(6) Rev. Eur. Econ. Pol'y 348 (2021); Jinghan Zeng et al., *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty,"* 45(3) Pol. & Pol'y 432 (2017).

8 Min Jiang & Luca Belli, *Contesting Digital Sovereignty: Untangling a Complex and Multifaceted Concept*, in Min Jiang & Luca Belli (eds.), Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance (2024).

made efforts to design a BRICS+ agenda for digital sovereignty. However, their focus is primarily on the development of cooperation in the spheres of digitalization and information security rather than on digital sovereignty itself. As a result, issues related to the pillars of digital sovereignty, analysis of existing regulations, and recommendations for BRICS+ to achieve sovereignty have been overlooked.

This paper aims to design a theoretical legal model of BRICS+ digital sovereignty, identify its pillars, and offer recommendations for BRICS+ to achieve digital sovereignty. To achieve this aim, we employed a set of methods. The comparative legal method was used to analyze regulations in digitalization and digital sovereignty among BRICS+ member countries. We also employed retrospective analysis to study the development of BRICS+ regulations in these areas. The systematic method enabled considering legal tools and instruments contributing to achieving digital sovereignty. The content analysis allowed the interpretation of grey literature, news articles and social media sources related to BRICS+ digital sovereignty.

The article begins with an introduction to the topic, substantiating its relevance and the necessity of researching BRICS+ digital sovereignty. Next, we focus on the concept of digital sovereignty and analyze the existing approaches to its definition and its key components. Next sections devoted to analysis of national legislation on digital sovereignty of BRICS+, and recommendations on how renewed alliance can ensure digital sovereignty on the BRICS+ level.

1. Digital Sovereignty Concept: Origin, Evolution, and Components

As previously mentioned, the concept of digital sovereignty remains controversial,[9] with scholars divided on whether it truly exists. The growth of digital networks in the 1990s made the disappearance of the state seem plausible, leading to the emergence of cyberspace sovereignty.

The growth of digital networks in the 1990s made the disappearance of the state an immediately plausible scenario, and the concept of the sovereignty of the cyberspace emerged.

Digital sovereignty can be traced back to John Perry Barlow's "Declaration of the Independence of Cyberspace,"[10] which asserted that governments have no authority in this ecosystem. Some researchers argue that the term "digital sovereignty" first entered the public domain in France through Pierre Bellanger in 2008 and was further defined in his 2014 book "La Souveraineté numérique."[11]

---

9 Robles-Carrillo 2023.

10 John P. Barlow, *A Declaration of the Independence of Cyberspace*, 18 Duke L. &Tech. Rev. 5 (2019).

11 *Digital Sovereignty and its Challenges: The Keys to Your Full Understanding*, Oodrive, 15 February 2022 (Jul. 1, 2024), available at https://www.oodrive.com/blog/actuality/digital-sovereignty-keys-full-understanding/.

However, many scholars contend that digital sovereignty does not exist. In 2020, Muller wrote "Against Sovereignty in Cyberspace," arguing that sovereignty in cyberspace is impossible. Conversely, in "In Defense of Pure Sovereignty in Cyberspace," K.J. Heller argued that such sovereignty does exist.

Notably, the initial concept of digital sovereignty as cyberspace independence from the state has changed drastically. Today, digital sovereignty is a powerful term in political discourse. It aims to reinstate the nation-state, including the national economy and its citizens, as relevant categories in the global governance of digital infrastructures and technologies. In other words, digital sovereignty has evolved from cyberspace sovereignty to a nation's sovereignty over its digital infrastructure and technologies.[12]. D. Grimm stated that digital sovereignty means

> the power to erect borders around incoming information, trade protectionism in the digital sector, and enhanced state power over the online accounts, data, and PII of its residents.[13]

Moreover, Pohle and Thiel expect the concept of digital sovereignty to gain even more political currency in the coming years.[14] Several related concepts include internet sovereignty, technological sovereignty, data sovereignty, and sovereign cloud.

The first two concepts are essentially synonymous, but data sovereignty is distinct. According to Chander and Sun, digital sovereignty

> should be defined broadly to encompass the sovereign power of a state to regulate not only the cross-border flow of data through the use of Internet filtering technologies and data localization mandates but also the activities of expression and access to technologies.[15]

Various sources indicate that data sovereignty

> relates to the rules and reference architectures that can help safeguard some of the fundamental principles of digital sovereignty: data storage, data jurisdiction, data protection, data independence and mobility, and data interoperability and portability.[16]

---

12 Julia Pohle & Thorsten Thiel, *Digital Sovereignty*, 9(4) Internet Policy Review (2020).

13 Dieter Grimm, *Sovereignty: The Origin and Future of a Political and Legal Concept* (2015).

14 Pohle & Thiel 2020.

15 Chander & Sun 2021.

16 Wenche Karlstad, *Explore the Path to Digital Sovereignty!*, Tietoevry, 17 May 2023 (Jul. 1, 2024), available at https://www.tietoevry.com/en/blog/2023/05/all-you-need-to-know-about-digital-sovereignty/.

Sovereign cloud, in turn, refers to

> a set of new and dynamic cross-/multi-cloud solutions designed to respond to new sovereign policies, balancing collaboration with compliance, and bringing together insight, innovation, growth, and security. It can be seen as an enabler of data sovereignty.[17]

Scholars and politicians need a unified understanding of the main pillars of digital sovereignty. For instance, the Joint Council of Ministers' decision on European digital sovereignty (7 April 2016) identifies three main pillars: 1) the capacity of EU Member States to defend their networks and reinforce their digital resilience; 2) the development of an autonomous, innovative industry, particularly in cybersecurity and trusted digital products; 3) the ability to decide autonomously on the level of security of their data, especially in the context of trade agreement negotiations.[18]

M. Mueller, on the other hand, defines the pillars of digital sovereignty as:

> 1) the power to erect borders around incoming information; 2) trade protectionism in the digital sector; 3) enhanced state power over the online accounts and data of its residents.[19]

According to E. Zinovieva and B. Yajie, the components of digital sovereignty include 1) the development of national search systems and social networks; 2) the strengthening of the digital contour of the national Internet segment, including the creation of data repositories and traffic exchange points.[20] Fang Binxing outlined four principles of digital sovereignty: 1) each country should have complete control over its segment of the Internet; 2) the state should be able to protect its segment from any external attacks; 3) all countries should have equal rights to using Internet resources; 4) other countries should have no control over the root DNS servers through which the national segment of the Internet is accessed.[21]

---

17 Karlstad, *supra* note 16.

18 *The European Digital Sovereignty – A Common Objective for France and Germany*, National Agency for Information Systems Security (Jul. 1, 2024), available at https://cyber.gouv.fr/en/actualites/european-digital-sovereignty-common-objective-france-and-germany.

19 Milton Mueller, *Digital Sovereignty: What Does It Mean?*, Internet Governance Project (Jul. 1, 2024), available at https://www.internetgovernance.org/wp-content/uploads/Digital-sovereignty-IGF2021.pdf.

20 *Digital Sovereignty in Russia and China*, Russian International Affairs Council, 14 June 2023 (Jul. 1, 2024), available at https://russiancouncil.ru/en/analytics-and-comments/analytics/digital-sovereignty-in-russia-and-china/.

21 *Мартиросян А.* Реалии цифрового суверенитета в современном мире // Журнал Международная жизнь [Arevik Martirosyan, *Realities of Digital Sovereignty in the Modern World*, International Life Journal] (Jul. 1, 2024), available at https://interaffairs.ru/jauthor/material/2483.

Analyzing these components, pillars, and principles of digital sovereignty allows us to identify the following constituents of digital sovereignty: 1) data protection; 2) cybersecurity; 3) efficient regulation through experimentation; 4) a favorable climate for technology development.

The first element, data protection, is essential for ensuring digital sovereignty. G. Vial stated that data represents "the new oil for the economy,"[22] highlighting the importance of adequate protection measures. While concerns about data protection often focus on government use, increasing worries center on how the private sector controls digital information.[23]

The second element, cybersecurity, is a crucial component of digital sovereignty due to its importance for national security, citizens, and the economy. Cybersecurity seeks to promote and ensure the overall security of digital information and information systems, aiming to secure the information society.[24]

Unlike the first two elements, the third and fourth cannot be considered traditional elements of digital sovereignty. As demonstrated, scholars focus mainly on data protection and cybersecurity, which are vital for ensuring digital sovereignty. However, the innovative nature of digital technologies, such as artificial intelligence[25] and quantum technologies, poses a significant challenge for regulators worldwide. Researchers argue that regulators must develop new approaches to digital technology regulation. Using regulatory sandboxes as experimental legal regimes is one way to test digital innovations' creation,[26] production, and implementation, making experimental regulation a sufficient element of digital sovereignty.

The final element, a favorable climate for technological development, is also crucial. Modern states often need more favorable conditions for developing innova-tive businesses,[27] hindering digitalization and achieving digital sovereignty. If states can effectively implement digital technologies, they can retain competitive advantages.[28] Generally, when states aim to achieve specific development goals, they apply special regulations or stimulating legal regimes, such as special economic zones and public-

---

22 Gregory Vial, *Understanding Digital Transformation: A Review and a Research Agenda*, 28(2) J. Strategic Inf. Syst. 118 (2019).

23 Stephen P. Mulligan & Chris D. Linebaugh, *Data Protection Law: An Overview* (March 2019) (Jul. 1, 2024), available at https://crsreports.congress.gov/product/pdf/R/R45631.

24 Uchenna J. Orji, *Cybersecurity Law and Regulation* (2012).

25 Damian Cyman et al., *Regulation of Artificial Intelligence in BRICS and the European Union*, 8(1) BRICS L.J. 86 (2021).

26 Elizaveta Gromova & Tjaša Ivanc, *Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS*, 7(2) BRICS L.J. 10 (2020).

27 Elizaveta Gromova & Daniel B. Ferreira, *Tools to Stimulate Blockchain: Application of Regulatory Sandboxes, Special Economic Zones, and Public Private Partnerships*, 2(1) Int'l J. L. in Chang. World 17 (2023).

28 Melanie Swan, *Blockchain: Blueprint for a New Economy* (2015).

private partnerships in digital technologies. A state must promote digital technologies using one or more of these regimes to succeed in achieving its goals.

2. Digital Sovereignty of BRICS Countries

The *Russian Federation* has taken several steps to ensure digital sovereignty. The Strategy for Scientific and Technological Development (28 February 2024) aims to achieve technological sovereignty by 2030, emphasizing cybersecurity and national security. The "Sovereign Internet Law" (Federal Law No. 90-FZ of 1 May 2019) established the legal foundations for a national internet traffic routing system and centralized management.[29] Data protection regulations are also being enhanced to protect various categories of personal data. Additionally, Russia uses experimental legal regimes (regulatory sandboxes) to create efficient regulations for digital technologies in areas ranging from fintech and unmanned vehicles to telemedicine and state governance.

The *People's Republic of China* is a pioneer in developing and implementing digital sovereignty. China's initial steps towards cyber and national security were taken in the 1990s by implementing the "Great Firewall." China has also enacted the Law on Cybersecurity and the National Cyberspace Security Strategy to ensure digital sovereignty and cybersecurity. The Data Security Law and the Personal Information Protection Law are critical legal documents introducing concepts like personal information, sensitive personal information, data processing, data security, and data risk control.[30]

However, China had started much earlier with other elements of digital sovereignty. Thus, Chinese special economic zones, famous across the globe as one of the reasons for the "Chinese economic miracle," emerged in the middle of the 1970s, which allowed the development of new technologies and a technology-based goods market and made China a renowned leader in this area.

China's approach to digital sovereignty emphasizes the importance of digital technologies for achieving geopolitical leadership, actively using regulatory sandboxes for efficient regulation in Fintech, Insurtech, and other markets. The legal framework for regulatory sandboxes began forming in 2016, and China now has several types of sandboxes to meet various market needs.

The *Republic of India* has also made strides in ensuring digital sovereignty. The Information Technology Act (2000)[31] was one of the initial steps, followed by the

---

29 Alena Epifanova, *Deciphering Russia's "Sovereign Internet Law,"* German Council on Foreign Relations (January 2020) (Jul. 1, 2024), available at https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

30 China – Data Protection Overview, DataGuidance (September 2024) (Sep. 10, 2024), available at https://www.dataguidance.com/notes/china-data-protection-overview.

31 Revati Prasad, *Bodies and Data: The Digital Sovereignty of the Indian State*, AoIR Selected Papers of Internet Research (2021).

National Cyber Security Policy (2013).[32] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) released in 2021 aimed to implement stricter rules for online platforms' content moderation and protect India's sovereignty and integrity.[33]

A key recommendation from the Working Group report dated 8 February 2018, was to implement a regulatory sandbox for the financial sector to improve efficiency, manage risks, and create new consumer opportunities. In line with this, the Reserve Bank of India introduced a draft regulatory framework for the regulatory sandbox on April 18, 2019.[34] India also offers a special tax regime for companies producing electronic components and semiconductors[35] and tax incentives for residents of special economic zones.[36]

The *Federative Republic of Brazil*. Digital sovereignty is low on the political agenda in Brazil. Becerra and Waisbord argued along similar lines in their recent article, noting that digital sovereignty has not been a recent concern for Latin American countries, which can be explained in part by the fact that "cybernationalism and sovereignty are tied to the geopolitics of the world's superpowers."[37]

However, it has made initial steps towards digital sovereignty and developed its cybersecurity strategy. The LGPD law, signed in recent years, aims to protect the data of Brazilian citizens and set strict information security standards. In June 2019, Brazil announced the creation of a regulatory sandbox to test business activities using new digital technologies, including blockchain, to foster the development of fintech and cryptocurrencies.

The *Republic of South Africa* does not emphasize digital sovereignty as much as its BRICS peers. The Protection of Personal Information Act (POPIA) was the first codification of common law principles related to data privacy, though not all of

---

32 *National Cyber Policy* (2013) (Jul. 1, 2024), available at https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.

33 *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules* (2021) (Jul. 1, 2024), available at https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf.

34 *Draft Enabling Framework for Regulatory Sandbox*, Reserve Bank of India, 18 April 2019 (Jul. 1, 2024), available at https://rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=920.

35 Scheme for Promotion of Manufacturing of Electric Components and Semi-Conductors (SPECS) in India, India Briefing (2020) (Jul. 1, 2024), available at https://www.india-briefing.com/doing-business-guide/india/taxation-and-accounting/tax-incentives-for-businesses#incentivesforelectronicmanufacturinginindiaHeader.

36 Incentives for Special Economic Zones (SEZs), India Briefing (Jul. 1, 2024), available at https://www.india-briefing.com/doing-business-guide/india/taxation-and-accounting/tax-incentives-for-businesses#incentivesforspecialeconomiczonessezsHeader.

37 Martin Becerra & Silvio R. Waisbord, *The Curious Absence of Cybernationalism in Latin America: Lessons for the Study of Digital Sovereignty and Governance*, 6(1-4) Comm. & Pub. 1 (2021).

its provisions are in force.[38] South Africa is developing strategies, policies, and regulations to define the increasingly important role of ICTs. For example, in April 2021, South Africa approved the National Data and Cloud Policy to promote data sovereignty and security.[39]

As mentioned earlier, unlike the five leading BRICS+ countries that can be recognized as "digital sovereignty hawks," the new countries lack the tools and mechanisms to achieve digital sovereignty.

In contrast, despite efforts to digitalize, the *Kingdom of Saudi Arabia* remains largely a consumer of digital technologies.[40] That might create severe problems for the way to BRICS+ digital sovereignty.

Though several efforts were made to foster technological advancements. Saudi Arabia is increasingly focusing on policies and strategies that enable the country to take a leadership position in the digital economy by encouraging investment and innovation in digital technologies. These policies include ICT Strategy (2023) to achieve Vision 2030 goals.

Saudi Arabia's ICT Sector Strategy 2019–2023 (ICT Strategy) was unveiled in August 2019 as an ambitious action plan to achieve multiple objectives: attracting leading international companies in emerging technologies, increasing the share of local content in the IT sector, and supporting coordination between relevant ICT organizations in the public and private sectors.[41]

The *Arab Republic of Egypt*. The ICT sector plays a critical role in Egypt's economy. Still, it faces regulatory hurdles that must be overcome to ensure its growth and continued contribution to the national economy. The local government must foster Internet accessibility, affordability, and quality of services to bridge the digital divide. Experts say it is due to the country's inconsistent Internet governance system, paved over arbitrary policies, overlapping jurisdictions and conflicting laws. A significant problem in Egypt is the lack of open, inclusive policy dialogue, perceivable through the Arab Internet Governance Forum. However, the Arab IGF ecosystem and the challenges of the regional process have prevented this from happening.[42]

---

38 *BRICS Countries Make Strides Towards Digital Sovereignty*, BRICS portal, 19 December 2019 (Jul. 1, 2024), available at https://infobrics.org/post/30020.

39 Jiang & Belli 2024.

40 Jad Haddad, *Saudi Arabia to Lead the Charge Toward Digital Sovereignty?*, Oliver Wyman, 1 June 2022 (Jul. 1, 2024), available at https://www.oliverwyman.com/our-expertise/insights/2022/jun/saudi-arabia-to-lead-the-charge-toward-digital-sovereignty.html.

41 *Country Review: Saudi Arabia's Digital Transformation and Collaborative Regulation*, International Telecommunication Union (2022) (Jul. 1, 2024), available at https://digitalregulation.org/wp-content/uploads/21-00770_R3_Saudi-Arabia-digital-transformation_E_web.pdf.

42 Noha Fathy, *Egypt*, National and Regional Internet Governance Forum Initiatives (NRIs), Global Information Society Watch (2017) (Jul. 1, 2024), available at https://giswatch.org/en/country-report/internet-governance/internet-governance-egypt-national-issues-roles-and-challenges.

United Arab Emirates. Unlike other new BRICS members, the United Arabian Emirates has made much more progress on the way to national digital sovereignty. In the United Arab Emirates (UAE), a legal landscape related to data sovereignty is gradually emerging. Although no legislation strictly regulates data sovereignty, several regulations address it. Two are Federal Law 45 of 2021, the Personal Data Protection Law (PDPL), and the Health Data Law. Experts state that the UAE's data protection[43] and cybersecurity[44] legislation is efficient and well-developed.[45] Moreover, the UAE is famous for its experimental regulation. Regulatory sandboxes for testing digital technologies in different areas, including RegTech, have been operating since 2016.[46] Moreover, several free zones[47] of the UAE offer special regimes of tax and other incentives for innovative businesses. All in all, the UAE can contribute to building BRICS+ digital sovereignty.

Federal Democratic Republic of Ethiopia. This BRICS+ member is currently just beginning to create regulation in the sphere of digital sovereignty. Thus, legislation in this area is being developed. For instance, there is a draft data protection regulation, but it has yet to be approved.[48]

The country also does not have developed legislation in the sphere of cybersecurity. However, Ethiopia has a New Cybercrime Law, though it introduced the first set of cybercrime rules with the enactment of the Criminal Code in 2004.[49]

Though Ethiopia has special economic zones that offer several incentives to a business, these zones aim to develop the agricultural sector rather than IT. The country also does not operate a regulatory sandbox but plans to have a legal framework and regulatory sandbox for central bank digital currency.[50]

---

43 *UAE adopts largest legislative reform in its history*, WAM (Jul. 1, 2024), available at https://www.wam.ae/en/details/1395302997239; Personal data protection law, https://ai.gov.ae/personal-data-protection-law/.

44 Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes, United Arab Emirates Legislations (Jul. 1, 2024), available at https://uaelegislation.gov.ae/en/legislations/1526.

45 Alaa Abouahmed et al., *Personal Data Protection in the United Arab Emirates and the European Union Regulations*, 13(1) J. Gov. & Reg. 195 (2024).

46 Regulatory sandboxes in the UAE, The Official Portal of the UAE Government (Jul. 1, 2024), available at https://u.ae/en/about-the-uae/digital-uae/regulatory-framework/regulatory-sandboxes-in-the-uae.

47 *Top Free Zones in UAE for Tech Startups: Your Ultimate Guide to Business Formation*, NH Management, 26 June 2024 (Jul. 1, 2024), available at https://nhmanagement.com/2024/06/26/top-free-zones-in-uae-for-tech-startups/.

48 Ethiopia – Data Protection Overview, DataGuidance (October 2023) (Jul. 1, 2024), available at https://www.dataguidance.com/notes/ethiopia-data-protection-overview.

49 Kinfe M. Yilma, *Comment: Some Remarks on Ethiopia's New Cybercrime Legislation*, 10(2) Mizan L. Rev. 448 (2016).

50 Derek Andersen, *Ethiopia Takes First Step Toward CBDC in Economic Reform*, Cointelegraph, 17 June 2024 (Jul. 1, 2024), available at https://cointelegraph.com/news/ethiopia-cbdc-economic-reform.

The *Islamic Republic of Iran* is working towards national digital sovereignty, with initiatives like a cybersecurity strategy and trade-industrial special economic zones offering tax incentives for industrial technology production. Launching a regulatory sandbox is on the Central Bank of Iran's agenda, but a draft of a regulatory framework is still needed.

In summary, BRICS+ countries possess significant digital development asymmetry, leading to varying distances from achieving digital sovereignty. While the five BRICS leaders and the UAE are more advanced on this path, other member states must catch up. This asymmetry poses an obstacle to BRICS digital sovereignty, but several recommendations outlined in the next section can diminish the asymmetry and achieve the BRICS+ digitalization goals.

3. On the Way to BRICS+ Digital Sovereignty

BRICS has consistently passed several legal acts that regulate vital aspects of digitization, including the Memorandum of Understanding on Cooperation in Science, Technology, and Innovation between the Governments of Brazil, Russia, India, China, and South Africa, approved in 2015 (from now on referred to as the Memorandum of Understanding)[51]; and the Strategy for BRICS Economic Partnership, also approved in 2015.[52] According to the Strategy for BRICS Economic Partnership, the BRICS strategy aims to enhance economic growth and competitiveness in the global arena. One of the main areas of BRICS cooperation is in the digital innovative economy. The Goa Declaration, approved at the 8th BRICS Summit 2016, also encourages digitization.[53] To further this goal, the Digital Economic Development Initiative was approved by the BRICS Business Council at the Xiamen Summit in 2018.[54]

These initiatives provide BRICS countries with the legal framework to promote cooperation in digital sovereignty. There is no doubt that BRICS+ has excellent potential to achieve digital sovereignty. However, asymmetry in the level of digitalization and its regulation presents obstacles. In the current geopolitical climate, it is imperative for BRICS+ to develop cooperation in digital sovereignty, making concerted efforts to overcome these challenges.

---

51 Memorandum of Understanding on Cooperation in Science, Technology and Innovation between the Governments of the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China and the Republic of South Africa, 18 June 2018 (Jul. 1, 2024), available at http://www.brics.utoronto.ca/docs/BRICS%20STI%20MoU%20ENGLISH.pdf.

52 The Strategy for BRICS Economic Partnership, 9 July 2015 (Jul. 1, 2024), available at http://www.brics.utoronto.ca/docs/150709-partnership-strategy-en.html.

53 8th BRICS Summit: Goa Declaration, 16 October 2016 (Jul. 1, 2024), available at http://www.brics.utoronto.ca/docs/161016-goa.html.

54 BRICS to prioritise digital economy – Survé, IOL, 4 April 2018 (Jul. 1, 2024), available at https://www.iol.co.za/business-report/economy/brics-to-prioritise-digital-economy-surve-14231613.

Therefore, it is crucial for BRICS+ to adopt a unified approach towards improving national regulations for digital technologies and strengthening their national innovation ecosystems. Simultaneously, BRICS+ must work together to ensure the digital sovereignty of the union itself. This necessitates the formulation of a comprehensive set of measures to ensure sovereignty.

Firstly, it is imperative to identify the authorized bodies that will participate in the working group to develop general recommendations on digital sovereignty for BRICS+. This step is crucial for the successful implementation of the proposed measures.

Secondly, the working group should draft a BRICS+ memorandum on digital sovereignty (perhaps called the Hawks Memorandum), outlining the agenda and action plan for achieving digital sovereignty.

Thirdly, BRICS+ should consider deploying a sovereign cloud to create an environment that helps organizations meet digital sovereignty requirements, including personal information protection.

Fourthly, to ensure BRICS+ digital sovereignty, member countries should develop a common currency that could substitute for the US dollar.

Fifthly, unifying the rules of the regulatory sandbox experimental legal regime could lead to establishing a BRICS+ Regulatory Sandbox. This step would create opportunities for cross-border testing of digital innovations in a safe environment, facilitating future exports and imports between BRICS+ members and other countries.

Notably, several countries have attempted to create a Global Regulatory Sandbox. The Global Regulatory Sandbox, or "Global Financial Innovation Network" (GFIN) initiative, was launched in 2018,[55] and at least 12 countries participated in the experimentation of financial technologies across borders.[56] However, the initiative was not successful due to the COVID-19 pandemic. Building on the Global Financial Innovation Network – GFIN idea, the BRICS+ regulatory sandbox would aim to create a network of regulators for information and knowledge sharing about innovation, joint policy work and regulatory trials, and cross-border innovations testing worldwide.

---

55 Global Financial Innovation Network (Jul. 1, 2024), available at https://www.thegfin.com/; Gromova & Ivanc 2020.

56 GFIN's members include Australian Securities & Investments Commission (ASIC), Hong Kong Monetary Authority (HKMA), Monetary Authority of Singapore (MAS), Consumer Financial Protection Bureau (CFPB) in the U.S., Bank of Lithuania, South African Reserve Bank (SARB), Abu Dhabi Global Market (ADGM) in the UAE, International Monetary Fund (IMF), and World Bank Group (Jul. 1, 2024), available at https://www.fintechfutures.com/2019/02/regulators-officially-launch-global-financial-innovation-network/#:~:text=GFIN%E2%80%99s%20members%20include%20Australian%20Securities,(IMF)%2C%20and%20World%20Bank%20Group.

Conclusion

BRICS has succeeded in consolidating positions on developing cooperation in ICTs, cybersecurity, and a digital governance regime based on respect for state sovereignty. The modern geopolitical situation necessitates strengthening collaboration and stimulating mutual efforts in BRICS+ digital sovereignty.

Despite several obstacles and barriers to achieving BRICS+ digital sovereignty, BRICS+ undoubtedly has the potential to become true "hawks of digital sovereignty."

The recommendations in this research article may help to achieve these goals and can be utilized in the policy and law-making processes of BRICS+ countries. The results of this research can serve as a foundation for further studies and contribute to the limited literature on the new BRICS.

Future research should delve into a comprehensive analysis of the national regulations on digital sovereignty in each BRICS+ member country. This in-depth understanding can help in formulating a robust model of national digital sovereignty, which can then be integrated into the overarching BRICS+ digital sovereignty model.

References

Abouahmed A. et al. *Personal Data Protection in the United Arab Emirates and the European Union Regulations*, 13(1) Journal of Governance & Regulation 195 (2024). https://doi.org/10.22495/jgrv13i1art17

Becerra M. & Waisbord S.R. *The Curious Absence of Cybernationalism in Latin America: Lessons for the Study of Digital Sovereignty and Governance*, 6(1-4) Communication and the Public 1 (2021). https://doi.org/10.1177/205704732110467

Budnitsky S. & Jia L. *Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance*, 21(5) European Journal of Cultural Studies 594 (2018). https://doi.org/10.1177/1367549417751151

Chander A. & Sun H. *Sovereignty 2.0* (2021). http://dx.doi.org/10.2139/ssrn.3904949

Crespi F. et al. *European Technological Sovereignty: An Emerging Framework for Policy Strategy*, 56(6) Review of European Economic Policy 348 (2021). https://doi.org/10.1007/s10272-021-1013-6

Cyman D. et al. *Regulation of Artificial Intelligence in BRICS and the European Union*, 8(1) BRICS Law Journal 86 (2021). https://doi.org/10.21684/2412-2343-2021-8-1-86-115

Elms D. *Digital Sovereignty: Protectionism or Autonomy* (2021).

Fabiano N. *Digital Sovereignty Between "Accountability" and the Value of Personal Data*, 5(3) Advances in Science, Technology and Engineering Systems Journal 270 (2020). https://doi.org/10.25046/aj050335

Ferreira D.B. & Gromova E.A. *Hyperrealistic Jurisprudence: The Digital Age and the (Un)Certainty of Judge Analytics*, 36 International Journal for the Semiotics of Law 2261 (2023). https://doi.org/10.1007/s11196-023-10015-0

Ferreira D.B. & Severo L. *Multiparty Mediation as Solution for Urban Conflicts: A Case Analysis from Brazil*, 8(3) BRICS Law Journal 5 (2021). https://doi.org/10.21684/2412-2343-2021-8-3-5-29

Ferreira D.B. et al. *Arbitration Chambers and Trust in Technology Provider: Impacts of Trust in Technology Intermediated Dispute Resolution Proceedings*, 68 Technology in Society 101872 (2022).

Grimm D. *Sovereignty: The Origin and Future of a Political and Legal Concept* (2015).

Gromova E. & Ivanc T. *Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS*, 7(2) BRICS Law Journal 10 (2020). https://doi.org/10.21684/2412-2343-2020-7-2-10-36

Gromova E.A. & Ferreira D.B. *Tools to Stimulate Blockchain: Application of Regulatory Sandboxes, Special Economic Zones, and Public Private Partnerships*, 2(1) International Journal of Law in Changing World 17 (2023). https://doi.org/10.54934/ijlcw.v2i1.48

Gromova E.A. et al. *ChatGPT and Other Intelligent Chatbots: Legal, Ethical and Dispute Resolution Concerns*, 5(10) Revista Brasileira de Alternative Dispute Resolution 153 (2023). https://doi.org/10.52028/rbadr.v5i10

Heller K.J. *In Defense of Pure Sovereignty in Cyberspace*, 97 International Law Studies 1432 (2021).

Min J. & Luca B. *Contesting Digital Sovereignty: Untangling a Complex and Multi-faceted Concept*, in Jiang M. & Belli L. (eds.), Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance (2024).

Mueller M.L. *Against Sovereignty in Cyberspace*, 22(4) International Studies Review 779 (2020). https:// doi.org/10.1093/isr/viz044

Orji U.J. *Cybersecurity Law and Regulation* (2012).

Pohle J. & Thiel T. *Digital Sovereignty*, 9(4) Internet Policy Review (2020). https://doi.org/10.14763/2020.4.1532

Posch R. *Digital Sovereignty and IT-Security for a Prosperous Society*, in Werthner H. & Van Harmelen F. (eds.), Informatics in the Future: Proceedings of the 11th European Computer Science Summit (2015). https://doi.org/10.1007/978-3-319-55735-9_7

Prasad R. *Bodies and Data: The Digital Sovereignty of the Indian State*, AoIR Selected Papers of Internet Research (2021). https://doi.org/10.5210/spir.v2021i0.12016

Roberts H. et al. *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, 10(3) Internet Policy Review (2021). https://doi.org/10.14763/2021.3.1575

Robles-Carrillo M. *Sovereignty vs. Digital Sovereignty*, 1(3) Journal of Digital Technologies and Law 673 (2023). https://doi.org/10.21202/jdtl.2023.29

Ruohonen J. *The Treachery of Images in the Digital Sovereignty Debate*, 31 Minds and Machines 439 (2021). https://doi.org/10.48550/arXiv.2012.02724

Solhchi M.A. & Baghbanno F. *Artificial Intelligence and its Role in the Development of the Future of Arbitration*, 2(2) International Journal of Law in Changing World 56 (2023). https://doi.org/10.54934/ijlcw.v2i2.56

Swan M. *Blockchain: Blueprint for a New Economy* (2015).

Yilma K.M. *Comment: Some Remarks on Ethiopia's New Cybercrime Legislation*, 10(2) Mizan Law Review 448 (2016).

Zeng J. et al. *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty,"* 45(3) Politics & Policy 432 (2017). https://doi.org/10.1111/polp.12202

Zetzsche D. et al. *Regulating a Revolution: From Regulatory Sandboxes to Smart Regu-\lation*, 23(1) Journal of Corporate & Financial Law 31 (2017). https://doi.org/10.2139/ssrn.3018534

Information about the authors

Elizaveta Gromova (Chelyabinsk, Russian Federation) – Associate Professor, Department of Business, Competition and Ecological Law, National Research University South Ural State University (78 Lenina Ave., Chelyabinsk, 454082, Russian Federation; e-mail: gromovaea@susu.ru) – **corresponding author**.

Daniel Brantes Ferreira (Kazan, Russian Federation) – Senior Researcher, Institute of Digital Technologies and Law, Kazan Innovative University named after V.G. Timiryasov, Professor, AMBRA University (Orlando, USA) (42 Moskovskaya St., Kazan, 420111, Russian Federation; e-mail: daniel.brantes@gmail.com).