Pre-print English version of BELLI L. Analysing the AI Sovereignty Debate through the Experience of BRICS Countries (以金砖国家经验解析人工智能主权) Chinese Journal of Cyberspace （《中国网信》杂志）, Issue No. 10 (2025). Presented at the Digital Economy Forum, World Internet Conference, 8th November 2025.

Analysing the AI Sovereignty Debate through the Experience of BRICS Countries

Luca Belli, Professor ate FGV Law School, Rio de Janeiro, Director of the Centre for Technology and Society at FGV.

Abstract

This paper examines the migration of the concept of digital sovereignty into the domain of artificial intelligence (AI) within the evolving framework of the BRICS and their recent expansion. Based on previous research developed by the author, AI sovereignty is considered as the prerogative and capacity of sovereign states to understand, develop and regulate AI systems, thus being able to govern digital assets and systems operating within their jurisdiction. This fundamental state attribution is consistent with principles of sovereign equality, non-intervention, and the right to self-determination of peoples, and has been progressively integrated in the BRICS. With the advent of AI, this prerogative acquires new dimensions, encompassing not only jurisdictional control over data and networks but also research, development and governance of algorithmic systems, compute infrastructures, and the legal architecture of automated decision-making. The paper traces this conceptual and regulatory migration from digital to AI sovereignty, highlighting the elements that must be considered as Key AI Sovereignty Enablers such as data, compute, algorithmic capacity, meaningful connectivity, electricity, digital literacy, cybersecurity and risk-based regulation. Through case studies of Brazil, Russia, India, China, and South Africa, as well as insights from newly acceding members, the analysis identifies diverse but convergent approaches to AI sovereignty. Critically, the enlargement of BRICS+ deepens legal pluralism in the grouping, while amplifying its bargaining power in international fora, increasing its possibility to shape an AI sovereignty model, balancing national prerogatives with collective co-determination of global digital order.

Keywords

Digital sovereignty; AI sovereignty; BRICS; digital governance; digital cooperation; multilateralism

1. Introduction: Why Digital Sovereignty is relevant in the BRICS Context?

Over the past decade, the term digital sovereignty has migrated from academic and think-tank analyses to diplomatic discourses and has acquired, more recently, a central place within legislative frameworks, regulatory regimes, and judicial reasoning. From a regulatory perspective, digital sovereignty expresses the prerogative and capacity of sovereign states to prescribe, adjudicate, and enforce norms governing digital assets and systems operating within their jurisdiction1. This fundamental state attribution is consistent with principles of sovereign equality, non-intervention, and the right to self-determination of peoples.[2] It can be seen as the natural continuation of classic notion of sovereignty[3], extending over socio-technical digital spaces – that are both territorial and transnational, material and virtual – the legitimate public authority as well as the state duty to protect and respect fundamental rights and provide effective remedies.

The BRICS grouping (Brazil, Russia, India, China, and South Africa, and the recent new members Egypt, Ethiopia, Indonesia, Iran, Saudi Arabia, and the United Arab Emirates) emerged along the 2000s as an informal grouping and evolved into a policy coordination forum for major emerging economies. Despite their diversity constitutional setups, political systems, economies, and legal traditions, BRICS members share strategic incentives for pursuing digital sovereignty: mitigating structural dependence on foreign technologies; preserving regulatory space tailored to the

[1] M Jiang and L Belli (eds), Digital Sovereignty from the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance (Cambridge University Press 2024).

[2] In this perspective, see for instance Belli L (2021) BRICS countries to build digital sovereignty. In: Belli, L. (Ed.). CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Cham: Springer. pp 271–280; Belli, L. (2023). Building good digital sovereignty through digital public infrastructures and digital commons in India and Brazil. G20's Think20 (T20). https://is.gd/BDCXss ; Belli et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano. FGV (2023); Belli, L. and Gaspar, W.B. (Eds.) The Quest for AI Sovereignty, Transparency and Accountability. Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition. Springer-Nature. (2025); Couture, S., & Toupin, S. (2019). What does the concept of "sovereignty" mean in digital, network and technological sovereignty? New Media & Society, 21(10), 2305–2322; Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4), 1–19.

[3] W. Shan, P. Simons and D. Singh. (Eds). Redefining Sovereignty in International Economic Law. Oxford: Hart Publishing 2008.

assertion of national values; advancing industrial and developmental objectives; and pluralizing global governance through the promotion of a multipolar order where Global Majority countries acquire stronger relevance and can be deemed as by the "locomotives forces of the South"[4]. In this perspective, digital sovereignty is not perceived as digital isolationism, repositioning it as a claim to co-determination in the international digital order that demands accommodation and combination of legal diversity, national sovereignty and autonomous development trajectories, to make them coexist peacefully and cooperatively in the global governance context[5].

Such rationale is even more relevant with regard to highly interdependent AI value chains where digital sovereignty claims necessarily need to be developed to foster coexistence. In this context, the BRICS institutionally integrate technology governance into summit and ministerial declarations and working groups covering science, technology, innovation, cybersecurity, and the data economy.[6] Domestically, each member iteratively adapts statutory frameworks regulation key issues such as data protection, cybersecurity, platform regulation, competition, and internet access to assert policy autonomy while enabling and regulating cross-border cooperation, data flows and trade. This orientation suggests a constitutive project to redesign digital governance architectures, diffusing agenda-setting power and embedding alternative models of authorities[7],

---

[4] In 1990, the Report of the South Commission, chaired by former Indian prime minister Manmohan Singh, who was a key figure in the establishment of the BRICS, called for the establishment of a South-South cooperation, stressing that "the emerging development patterns of the North clearly suggest that the Northern locomotive economies will not pull the train of Southern economies at a pace that will satisfy its passengers-the people of the South. The locomotive power has to be generated to the maximum extent possible within the economies of the South themselves." See The South Commission. The Challenge to the South: The Report of the South Commission. Oxford University Press. (1990) p.286; Belli, L. BRICS: The New Digital Locomotives. Beijing Review. (11 July 2022). https://www.bjreview.com/Opinion/Voice/202207/t20220711_800300500.html

[5] L Belli, 'BRICS countries and AI sovereignty: Introduction to Thematic Section' (2024) 34 African Journal of Information and Communication.

[6] An ample range of research outputs mapping these issues, developed by the CyberBRICS project hosted by the Center for Technology and Society at FGV, is freely available on www.cyberbrics.info

[7] M Jiang and L Belli (eds), ibid.

particularly salient given the group's recent enlargement encompassing Egypt, Ethiopia, Iran, the UAE, and Indonesia, with Saudi Arabia's membership still pending at the time of this writing[8].

The inclusion of new members introduces further economic interests, political diversity and legal pluralism. Hence, the expanded BRICS+ face an increasingly complex normative scenario internally on digital and AI issues, while offering an opportunity to enhance cooperation, shaping coordinated sovereign governance mechanisms, across diverse sectors[9].

2. From Digital Sovereignty to AI Sovereignty: Conceptual Foundations

The AI sovereignty debates build upon and extend the ongoing digital sovereignty discussions. As articulated in previous publication.[10] The concept of AI Sovereignty was coined by Belli (2023) and defined as "a given country's capacity to understand, muster and develop AI systems, while retaining control, agency, and ultimately, self-determination over such systems"[11]. Hence, AI sovereignty aims at maximizing the use and development of AI systems for the promotion of national interest and values, while reducing – and ideally eliminating – that the use of foreign AI might lead to technological dependencies and power asymmetries. After being presented at Carnegie Digital Democracy Network Conference and at the UN Internet Governance Forum (IGF), respectively in May and October 2023, this concept rapidly became fashionable especially – and, to some extent, surprisingly – within US industry circles.

---

[8] Reuters, 'BRICS welcomes new members in push to reshuffle world order' (24 August 2023) https://www.reuters.com/world/brics-poised-invite-new-members-join-bloc-sources-2023-08-24/ accessed 27 August 2025.
[9] Ibid; see also Council on Foreign Relations, 'What Is the BRICS Group and Why Is It Expanding?' (2024) https://www.cfr.org/backgrounder/what-brics-group-and-why-it-expanding?utm_source=chatgpt.com accessed 27 August 2025.
[10] See nots 1, 2, 5 and 6.
[11] See Belli, L. To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE) p.23, in Feldstein S. (Ed.) (2023). Return to New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms. Carnegie Endowment for International Peace.

Notably, after the presentation of the first volume on AI Sovereignty[12] at the UN Internet Governance Forum, in October 2023, multiple AI companies have enthusiastically adopted the AI sovereignty term and starting to brand their products as ideal solutions to become AI sovereign. Particularly telling examples have appeared, since early 2024, on the websites of NVIDIA and Oracle, two large AI equipment vendors, which published blogposts dedicated to "explaining" what AI Sovereignty is, arguing that governments merely need purchasing their products and services to become AI sovereign.[13]

This corporate vision of AI sovereignty may not be completely objective. As noted by Belli (2023) being AI sovereign requires recognising the essential role of research, development, governance and regulation with regards to at least eight Key AI Sovereignty Enablers (KASE): i) personal and non-personal data, ii) software and algorithmic models, iii) computational capacity, iv) meaningful connectivity, v) electric power, vi) digital literacy, vii) cybersecurity and viii) AI-related risk management. These elements are all equally important and interconnected and neglecting one or more may likely lead to create vulnerabilities in the entire AI Sovereignty Stack or failing to appropriately cope with existing vulnerabilities.

The KASE framework, exposed by Belli (2023), is briefly presented below hoping it can positively inspire policymakers and other stakeholders alike in their understanding of AI sovereignty.

---

[12] The first version of the volume dedicated to "The Quest for AI Sovereignty, Transparency and Accountability" was presented at the UN IGF in Kyoto Japan in October 2023, and is available on the Forum website https://www.intgovforum.org/en/filedepot_download/288/26421

[13] Nvidia's blog states that "Sovereign AI refers to a nation's capabilities to produce artificial intelligence using its own infrastructure, data, workforce and business networks" adding that "[s]ince 2019, NVIDIA's AI Nations initiative has helped countries spanning every region of the globe to build sovereign AI capabilities." See Keith Strier. What Is Sovereign AI? NVIDIA's blog. (28 February 2024). https://blogs.nvidia.com/blog/what-is-sovereign-ai/ For Oracle, the very definition of Sovereign AI entails being a customer of its cloud computing services, as it succinctly states: "Achieve AI sovereignty with increased control over where you run your AI workloads and how you manage data and operate infrastructure with Oracle AI and Oracle Cloud Infrastructure (OCI) distributed cloud solution." See Oracle. Sovereign AI. Oracle's Cloud and Artificial Intelligence Blog. (s.d.) https://www.oracle.com/artificial-intelligence/sovereign-ai/

i) Personal and Non-Personal Data: Being able to construct solid data sovereignty, considered as "the capacity to understand how and why (personal) data are processed and by whom, develop data processing capabilities, and effectively regulate data processing, thus retaining self-determination and control"[14] is an essential component of AI sovereignty. Particularly, being able to have access to high-quality, diverse, and ethically sourced data is fundamental for training and improving AI models. Sovereignty over data allows nations to protect citizens' privacy, ensure data security, and regulate the use of sensitive information, thereby maintaining control over the development of AI systems, that reflect their cultural and societal norms, rather than being regulated by such systems.

ii) Software and algorithmic models are the foundation of AI systems, enabling machines to perform tasks and make decisions. Importantly, algorithm development, deployment, and regulation are all equally important dimensions of algorithmic governance and algorithmic models can be both the subject and facilitator of regulation. By investing in algorithmic research and development (R&D), and crating sound policies and regulations, nations can develop cutting-edge algorithms that enable more accurate, efficient, and adaptable AI systems. This, in turn, empowers them to maintain a competitive edge in the global AI market, drive economic growth, and address pressing societal challenges. Furthermore, R&D on algorithmic models allows nations to tailor AI technologies to their specific needs and values, ensuring that AI systems align with their cultural, ethical, and legal frameworks. This is particularly important in domains such as healthcare, finance, and public policy, where the responsible and fair use of AI is paramount. By investing in R&D, nations can develop algorithms that are transparent, explainable, and

[14] Belli L., Gaspar, W.B., Singh Jaswant, S. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. Computer Law & Security Review. Special issue on Digital Transformation in the BRICS Countries. Volume 54. (2024). https://doi.org/10.1016/j.clsr.2024.106017

accountable, thereby building public trust and facilitating the sustainable adoption of AI technologies.

iii) Computational Capacity: Training complex AI models and processing large datasets require substantial computational resources. Particularly, the most advanced AI systems, such as generative AI, can be remarkably computer-intensive due to their increased complexity. Ensuring the availability of sufficient computational capacity is critical for training and running complex AI systems. By investing in computational infrastructure, and regulating it in order to avoid concentration, nations can reduce dependence on external providers, accelerate AI research and development, and foster the growth of AI industries[15].

iv) Meaningful Connectivity: Reliable, well-performing, universally accessible internet infrastructure for an affordable price is essential for the deployment and operation of AI systems. Seamless connectivity facilitates data exchange, collaboration, and access to cloud-based AI services. It enables real-time applications and supports the development and deployment of AI technologies across sectors, contributing to the construction of a country's AI sovereignty.

v) Electric Power: AI systems require significant amounts of energy to operate, making access to reliable and sustainable power sources crucial. As AI systems grow in relevance and size, they require a stable and robust supply of electrical power to operate effectively. Ensuring the sustainability and reliability of power infrastructure is necessary for maintaining uninterrupted AI operations. By investing in renewable energy infrastructure, nations can support the growth of their AI industries, reduce carbon emissions, and ensure the long-term viability of AI applications.

[15] Vipra, J. & Myers West, S. Computational Power and AI. AI Now Institute. (2023) https://ainowinstitute.org/publication/policy/compute-and-ai

vi) Digital literacy: Enhancing the digital literacy of the population through capacity building, training, and multigenerational education is essential not only to achieving a skilled AI workforce but also to fostering cybersecurity and, ultimately, national sovereignty. Developing a skilled workforce capable of designing, building, and deploying AI systems is particularly crucial. Hence, the objective of AI capacity building should be to cultivate and retain a talent pool that can drive innovation and competitiveness in the global AI market.

vii) Cybersecurity: The importance of cybersecurity cannot be overstated. AI systems are susceptible to cybersecurity threats and can be used to perpetrate cyber-attacks, and AI critical infrastructure can come under attack. Indeed, AI can be leveraged by organisations to enhance their cyber defences, it can also be exploited by cybercriminals to launch targeted attacks at an unprecedented speed and scale, bypassing traditional detection measures[16]. As AI systems become increasingly integrated into critical infrastructure, ensuring their security against cyber threats is paramount. Robust cybersecurity measures help protect AI assets, maintain public trust, and prevent the misuse of AI technologies for malicious purposes.

viii) AI-Related Risks: A comprehensive governance framework that addresses AI-related risks[17], encompassing ethical considerations, data protection laws, and risk-management tools is crucial for AI sovereignty. However, as we will stress, risk-based regulation is necessary but not sufficient to frame AI. Managing the ethical, legal, and societal implications of AI is essential for maintaining public support and ensuring the responsible development and deployment of AI systems. By establishing

[16] Belli, L., Gaspar W.B., et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano. FGV Direito Rio. (2023). https://repositorio.fgv.br/items/4814c750-6b42-4d48-b8bb-302ce467b4ea; Belli L. "When AI Meets Cybersecurity: Framing Brazil’s Information Security and AI Challenges” in Feldstein S. (Ed). Digital Democracy in a Divided Global Landscape. Carnegie Endowment for International Peace. (2025).

[17] Slattery P. et al. The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks From Artificial Intelligence. Massachusetts Institute of Technology. (2024).

clear regulatory frameworks and, crucially, promoting transparency and accountability, nations can mitigate potential risks and harness the benefits of AI in a way that aligns with their fundamental values and priorities.

Importantly, the abovementioned Key AI Sovereignty Enablers must be considered as interdependent, forming an AI Sovereignty Stack, which plays an instrumental role to determine a nation's ability to leverage AI for economic, social, and strategic advantage. By investing in these enablers, nations can reassert their sovereignty on AI technology, establishing a solid foundation for AI development, safeguarding their interests, shaping the evolution and adoption of AI in a way that promotes and preserves their values.

Furthermore, is important to emphasise that the implementation of the KASE framework does not aim at fostering AI autarchy. On the contrary, it means being able to understand how AI system works and the impact they might have to be able to define one's digital future, while cooperating with as many partners as possible, to increase trade and cooperation on fair terms and avoid being technologically dependent. This approach will allow us to discuss how nations in the Global South are striving to navigate the complexities of AI governance, to avoid becoming or continuing to be digital colonies[18], forging innovative paths to harness the transformative potential of AI while safeguarding their interests and values.

3. Lessons from Selected BRICS Jurisdictions

18 The concept of digital colonialism is explored by an increasing number of authors. See e.g. 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; 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; Benyera, E. (2021). The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data. Routledge.

Within the BRICS context, each member has sought to articulate a distinctive approach to AI governance and, consequently, AI sovereignty that reflects its institutional capacities, political economy, and normative priorities. While their trajectories differ, all are united by a common concern with safeguarding autonomy in the face of global technological dependencies, especially those linked to data flows, computational infrastructures, and algorithmic models. The commitment to AI sovereignty is not merely a matter of protecting domestic industries, but rather an attempt to assert a legal and political capacity to regulate, direct, and benefit from AI in ways that serve national development strategies and reinforce state legitimacy.

By examining the national experiences of the founding members —Brazil, Russia, India, China, and South Africa— it is possible to observe how different models of AI sovereignty are emerging within the expanded grouping. Together, these experiences provide a comparative basis for understanding how AI sovereignty is framed, regulated, and operationalized across diverse political systems, and how BRICS as a collective can contribute to shaping the normative foundations of global AI governance.

3.1. Brazil: Development-Oriented AI Sovereignty

The Brazilian AI Plan *(PBIA)*, announced in 2024 adopted in 2035 operates as a policy blueprint, affirming commitments to human-centric, transparent, explainable, and non-discriminatory AI development, linked to productivity gains, inclusive growth, and regional leadership aspirations[19]. While not codified law, PBIA harnesses existing statutory and institutional anchors to foreground investment in research infrastructure, compute resources, talent development, procurement-driven innovation in public administration, international standard alignment, and ethical principles operationalised through guidelines and sectoral rules.

[19] Johansson Neto G, Farias da Costa V and Gaspar W, 'Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI sovereignty?' (2024) 34 African Journal of Information and Communication 35.

However, despite progress, financing and governance coherence remain challenges for Brazil. A robust compute-strategy is evolving, including incentives for regional cloud nodes and semiconductor policy. The institutional capacity – both as regards implementing industrial policy and enforcing existing or proposed AI related norms – will play a pivotal role for the success of the Brazilian approach.

3.2. Russia: Securitized AI Sovereignty

Russia's approach to AI has a strong focus on security, emphasizing strategic autonomy, information control, and defense modernization, with an integrated military-civil industrial synergy. Public investment primarily underwrites enterprises and research institutions that foster national interest, with stringent data flow controls under national protection and cybersecurity regulations.[20].

This approach maximizes control over strategic assets but risks limiting civilian innovation and international academic and commercial collaboration, which are already reduced due to sanctions and export controls. Moreover, attention to AI liability and consumer protections may be underdeveloped as security law predominates over administrative and private law accountability. In this perspective, Russia typifies the security-first ideal-type in the BRICS AI sovereignty spectrum[21].

3.3. India: Developmental Promise Amid Fragmentation

As aptly stressed by Vipra, India's AI sovereignty can be seen as tripartite construct based on: deployment of AI for governance and development (e.g., agriculture, health, disaster management); institutional fragmentation and multiplicity of overlapping regulations and

[20] A Ignatov and D Kerimi, 'Russia's securitized approach to AI sovereignty' (2024) 34 African Journal of Information and Communication 58.
[21] Ibid.

ministries; and the rapid expansion of both Digital Public Infrastructures[22]. - including Aadhaar, UPI, and the DEPA in the context of the India Stack digital transformation program - and surveillance technologies.[23]

One of India's greatest asset is to benefit from a large digital entrepreneurship and data science ecosystem, but suffers from a still nascent and not yet streamlined rights-preserving framework, and dependence on foreign compute. Hence, in the Indian context, strengthening sovereignty entails consolidating institutional mandates, implementing enforceable AI-regulation, and leveraging state procurement to require auditable, interoperable AI models[24].

3.4. China: Dual-Track Regulatory Strategy

China's AI sovereignty features a dualistic regulatory structure combining strong regulatory frameworks, in areas such as content moderation, cybersecurity, algorithmic transparency and data protection[25], with facilitative industrial policies promoting extensive R&D investment, AI pilot zones, and national computing hubs[26].

Political and social stability are national priorities driving the regulation of AI through ex ante controls, while the state plays a pivotal role in the promotion and support of entrepreneurship, fostering innovation ecosystems. This model reduces extraterritorial corporate reliance, prioritizing industrial expansion and security, thus reducing technological dependencies and systemic vulnerabilities.

[22] A Sengupta, AC Barbosa and M Samdub, 'Understanding interrelationships between AI and digital public infrastructure in India and Brazil' (2024) 34 African Journal of Information and Communication 82.
[23] J Vipra, 'Towards AI sovereignty: The good, the bad, and the ugly of AI policy in India' (2024) 34 African Journal of Information and Communication 101.
[24] Ibid.
[25] Wang, Wayne Wei et al., Artificial Intelligence "Law(s)" in China: Retrospect and Prospect (November 30, 2024). Part I, Journal of AI Law and Regulation (AIRe), Vol. 2, No. 1, pp. 29-36, 2025 & Part II, Journal of AI Law and Regulation (AIRe), Vol. 2, No. 2, pp. 139-157, 2025.
[26] A Ma, 'Regulation in pursuit of artificial intelligence (AI) sovereignty: China's mix of restrictive and facilitative modalities' (2024) 34 African Journal of Information and Communication 120.

3.5. South Africa's hybrid approach

South Africa presents a distinctive hybrid approach to AI sovereignty, combining strong normative commitments to rights-based governance with pragmatic strategies for fostering innovation and economic competitiveness. As Musoni and Snail argue, the South African framework for AI development is deeply rooted in constitutional principles that privilege the protection of human dignity, equality, and freedom, which in turn influence the design of regulatory and institutional enablers of AI sovereignty.[27] This rights-based orientation is particularly evident in the implementation of the Protection of Personal Information Act, which establishes a robust legal foundation for data protection and, by extension, for national control over the flows and uses of personal information in AI systems.

At the same time, South Africa's policy discourse acknowledges the need to stimulate domestic innovation ecosystems, including public–private partnerships, research institutions, and open data initiatives, which are seen as essential for ensuring that AI sovereignty translates into both autonomy and developmental benefits. The hybrid character of South Africa's approach lies in its dual emphasis on regulatory sovereignty and innovation-driven growth.

4. Conclusion: BRICS Collective Trajectories for collaborative AI Sovereignty

Since the mid-2010s, BRICS have evolved from declaratory digital governance statements to operational initiatives in research collaboration, shared standardization, and capacity-building. The group has acquired a critical role as a policy space for diverse national AI governance models united by development and sovereignty commitments, rather than imposing uniformity[28]. In this

[27] Melody Musoni and Sizwe Snail ka Mtuze. 'An Assessment of the Key AI Sovereignty Enablers within the South African Context' in Belli L. Gaspar. W.B. The Quest for AI Sovereignty, Transparency and Accountability. Springer-Nature. (2025).

[28] L Belli, 'How are BRICS countries building AI sovereignty? Introduction to Thematic Section' (2025) 35 African Journal of Information and Communication 1.

context, BRICS has actively promoted sovereign equality, non-discrimination in technology transfer, and the right to benefit from scientific progress, translating into demands for equitable compute access, standards participation, and both technological and regulatory autonomy. The BRICS Leaders' Statement on Global Governance of Artificial Intelligence[29] can be seen as a landmark document in an evolving AI sovereignty narrative, as it highlights the urgency of implementing safeguards – such as data rights, accountability mechanisms, and equitable value distribution – to promote a sustainable AI ecosystem.

The expansion towards a BRICS+ configuration, including Egypt, Ethiopia, Iran, UAE, and Indonesia, has increased the not only the group's scale and heterogeneity, but also its economic heft and international bargaining weight. Nonetheless, a pragmatic approach suggest to consider also the challenges that lie ahead. External pressures such as export controls, sanctions, and geopolitical instability may jeopardize global cooperation and research partnerships and, more concretely, restrict access to computational resource. However, such challenges should also be seen as opportunities as necessity is the mother of invention. In this spirit, BRICS have an opportunity to foster resilience through indigenous R&D enhancement, supply diversification, pooled procurement, and promotion of open-source AI[30].

BRICS AI sovereignty experiences epitomize that digital policy and governance evolve as a living ecosystem, which is increasingly driven by Global Majority leaders.[31] In this perspective, the intrinsic legal and geopolitical pluralism of BRICS can be seen as an asset rather than an obstacle, forming a laboratory for AI governance designs and policy proposals, that can be iterated and transposed across jurisdictions.

[29] BRICS. BRICS Leaders' Statement on the Global Governance of Artificial Intelligence. (July 2025). https://cyberbrics.info/brics-leaders-statement-onthe-global-governance-of-artificial-intelligence/
[30] Belli 2023, 2024.
[31] M Jiang and L Belli (eds), (n 1).