BRICS countries and AI sovereignty: Introduction to Thematic Section

Luca Belli
Professor of Law and Director of Center for Technology and Society (CTS) and CyberBRICS project, Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro
https://orcid.org/0000-0002-9997-2998

Keywords
artificial intelligence (AI), AI sovereignty, digital sovereignty, BRICS

DOI: https://doi.org/10.23962/ajic.i34.128842

Recommended citation
Belli, L. (2024). BRICS countries and AI sovereignty: Introduction to Thematic Sectio. *The African Journal of Information and Communication (AJIC)*, *34,* 1-6. https://doi.org/10.23962/ajic.i34.128842

1. Introduction

Artificial intelligence (AI) has emerged as a transformative force that is reshaping economies, political landscapes, societal interactions and, most evidently, narratives around technology. In this context, this Thematic Section of *The African Journal of Information and Communication (AJIC)* includes the first two products—one from China (by Aifang Ma), and one from Brazil (by Germano Johansson Neto, Viviane Farias da Costa, and Walter Britto Gaspar)—of the ongoing research we at the CyberBRICS project are conducting on AI sovereignty in the BRICS countries.

The CyberBRICS project,[1] hosted since 2018 by the Center for Technology and Society (CTS) at FGV Law School in Rio de Janeiro is a multidisciplinary research programme dedicated to analysis of digital policies in the BRICS countries.[2] CyberBRICS and *AJIC* share the goal of publishing high-quality and impactful research on crucial digital issues affecting the Global South and promoting analyses that reflect the perspectives of leading Global Southern countries. Our current focus at CyberBRICS, on the various facets of AI sovereignty, builds upon the previous phases

1 See https://cyberbrics.info
2 At present in late 2024, there are nine BRICS countries: Brazil, Russia, India, China, South Africa, Iran, Egypt, Ethiopia, and the United Arab Emirates.

of our research, which were dedicated to cybersecurity, data governance, digital transformation, and digital sovereignty. In this introductory piece, I seek to provide the reader with some background necessary to understand the reasoning behind our current focus on the quest for AI sovereignty in the BRICS. The sections that follow set out some of the key rationales guiding this current research agenda.

2. What is AI sovereignty?

The two articles that follow in this Thematic Section adopt a working definition of "AI sovereignty" based on the key AI sovereignty enablers (KASE) framework set out in Belli (2023b), in which AI sovereignty is cast as the ability to understand, develop, and regulate AI systems in order to exercise self-determination, agency, and control over such systems. Such definition represents an evolution of the concept of "digital sovereignty", which we have previously defined as "the capacity to exercise agency, power and control in shaping digital infrastructure, data, services, and protocols" (Jiang & Belli, 2024, p.7. The KASE framework identifies the essential elements that a country's AI research and development (R&D), governance, and regulation must pursue if the country is to achieve a full "AI sovereignty stack", which is "a layered structure" that reduces "the country's exposure to the technological choices of foreign (private or public) actors" and enhances the country's "agency and self-determination" with respect to deployment of AI systems (Belli, 2023b, p. 1).

In the KASE framework, the AI sovereignty enablers are (Belli, 2023b, p. 2): "sound (personal) data governance and algorithmic governance, strong computational capacity, meaningful connectivity, reliable electrical power, a digitally literate population, solid cybersecurity, and last, but not least, an appropriate regulatory framework" dedicated to AI risks. To these foundational elements, our ongoing analysis has added examination of how digital public infrastructures (DPIs) are used to support AI systems and, conversely, how AI systems can be leveraged to support DPIs.

As discussed in numerous CyberBRICS research outputs,[3] the BRICS countries' approaches to digital sovereignty in general and, more recently, to AI sovereignty, vary enormously as regards their rationale and structure, and have been motivated by multiple and diverse perspectives. These perspectives span from being fully aware (due to the colonial past of most of the group members) of the consequences of technological dependence, to seeing the need to leverage domestic innovation to

3 CyberBRICS publications are available on an open access basis at https://cyberbrics.info/cyber-brics-publications

spur development and build "technological autonomy"[4] in line with their well-rooted developmentalist traditions. The BRICS countries' perspectives also include the understanding that digital technologies and AI systems can be leveraged either to undermine or to reassert the essence of their constitutional frameworks, thus directly impacting state sovereignty, individual rights, and national economies. Also clearly understood by the BRICS is the necessity to cope with increasingly relevant geopolitical tensions, which have led to mounting suspicions, protectionism, and explicit sanctions targeting digital products and services (and thus disrupting digital supply chains) (Belli & Galdino de Magalhães, 2024).

The CyberBRICS project's analyses of AI sovereignty dynamics stem from the consideration that the classical concept of sovereignty, rooted in the nation-state, has faced significant disruption in recent decades and fails to consider the emergence of an additional layer of "private sovereignty" (Belli, 2022). This has been established by the widespread adoption of borderless digital technologies and AI systems that have local implications through directly shaping the rights, interests and behaviours of both physical and juridical persons based in the multiple countries where such systems are utilised.

Historically defined as supreme authority within territorial boundaries (as articulated by thinkers like Jean Bodin and codified in the 1648 Peace of Westphalia), sovereignty today contends with new challenges, tellingly illustrated by the prevailing technological dependencies and new extractive practices, defined by several authors as "digital colonialism" or "data colonialism" (see, for example, Avila Pinto, 2018; Couldry & Mejias, 2019; Benyera, 2021). In this perspective, the adoption of AI system has enabled new private actors to wield quasi-sovereign powers through defining the ways in which people, corporations, and states can interact through the structures of their systems—thus providing vivid illustrations of what Strange (1988) defines as "structural power" and Lessig (1999; 2006) has called regulation by "architecture".

Hence, the AI sovereignty debate can be situated at the nexus of regulatory, governance, market, and infrastructural dynamics—a nexus that demands a systemic approach in order to comprehend its implications fully. While sovereignty traditionally emphasised independence from external control, AI sovereignty hinges on the ability of technology—particularly AI—to shape and regulate behaviours of physical and juridical persons, including states, through structural power. To ascertain the extent to which entities can be deemed as AI sovereign requires full understanding of the

4 Article 219 of Brazil's Constitution considers "technological autonomy" as a constitutional objective, thus giving a constitutional law base to the pursuit of digital and AI sovereignty in the country. See https://www.stf.jus.br/arquivo/cms/legislacaoConstituicao/anexo/brazil_federal_constitution.pdf

interconnectedness and interplay among the several AI sovereignty enablers, as set out in the KASE framework—a framework we have deployed in order conduct country studies (two of which, on the Chinese and Brazilian national contexts, are drawn on in this Thematic Section), and comparative work across the BRICS countries.

3. Why the BRICS?

Probably the only element of agreement amongst various BRICS observers is that the grouping is unusual in nature. The term "BRICs", coined by O'Neill (2001) to identify the leading emerging economies with the strongest growth projection by 2030, has since evolved into an alliance representing an increasing number of voices and interests in the Global South. In 2024, the grouping added four new members—Egypt, Ethiopia, Iran, and the United Arab Emirates—and approximately 40 other nations have expressed interest in joining, reflecting the bloc's growing influence.

The development of this group reflects a broader historical trajectory of emerging economies striving to create Global South-led alternatives to Western-centric global governance structures that have been established by former colonial powers and that perpetrate neocolonial interests. The enlargement of BRICS underscores developing countries' increasing dissatisfaction with a perceived double standard in international relationships and their widespread desire, as the global majority, to forge a multipolar international order where multiple options are available and former colonies do not depend on former colonisers. In this sense, the notions of AI sovereignty and digital sovereignty do not need to be seen as synonyms for AI autarchy or digital autarchy, but rather as notions implying the capacity to be technologically autonomous and free to cooperate with no strings attached.

Emerging economies are drawn to BRICS by the increasing attractiveness of the members' economies as well as by the grouping's potential to balance global power dynamics and provide a platform to address shared challenges, including with respect to digital matters. A case in point in this regard is the new Convention on Cybercrime, which was adopted by consensus at the UN and was strongly supported by the BRICS (UN General Assembly, 2024). This Convention was proposed by Russia and China, backed by India, and brokered thanks to the efforts of Brazil and, to a much lesser extent, South Africa. The Convention emerged from a decade of intense scrutiny of cybersecurity issues spurred by the 2013 revelations of former US National Security Agency (NSA) contractor Edward Snowden (Belli, 2021a, 2021b; Belli et al., 2023). This Convention is perhaps one of the greatest achievements to date of the coordination and joint action of BRICS leaders with regard to digital policies—notwithstanding the criticisms that can legitimately be raised about the content of the Convention, whose scope is so broad that it could facilitate surveillance and repression.

Only five years ago, the thought that a cybercrime treaty proposed and supported by BRICS countries could be adopted by the UN was not taken seriously by the vast majority of observers. Recent geopolitical developments seem to have markedly redefined the relevance of the BRICS as a club-governance mechanism, thus opening a new chapter in the pursuit of global multipolarity.

4. Conclusion

As countries vie for technological supremacy, issues of technological dependency and autonomy become increasingly relevant. The CyberBRICS project's approach to AI sovereignty is grounded in the understanding that achieving such sovereignty is not only about technological or regulatory capabilities but also about asserting agency and self-determination over (and through) AI systems, all within a highly opaque and concentrated global technological landscape (Belli, 2023a; 2023b; Belli, et al. 2023: Belli & Galdino de Magalhães, 2024; Jiang and Belli, 2024).

The two contributions that follow in this Thematic Section provide initial yet valuable insights into how two of the founding BRICS countries, China and Brazil, are building and implementing their strategic approaches to AI sovereignty—with, in both countries, AI linked to technological, economic, and national self-determination objectives. For the BRICS countries and other emerging economies, achieving AI sovereignty involves navigating complex interdependencies, addressing infrastructural gaps, and fostering innovation, including innovation in regulation, e.g., through understanding that providing market incentives and building out technological infrastructures are forms of regulation. By embracing a systemic approach that integrates governance, regulation, and industrial policy, nations can establish agency over AI systems and shape their futures in the global digital economy. As the two articles that follow demonstrate, the journey towards AI sovereignty is both challenging and imperative. It is only through systemic, multidimensional and multistakeholder approaches, focused on achieving concrete results through implementation of strategic objectives, that nations can fully harness the transformative power of AI while safeguarding national sovereignty and independence.

References

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.

Belli, L. (Ed.). (2021a). *CyberBRICS: Cybersecurity regulations in the BRICS countries.* Springer. https://doi.org/10.1007/978-3-030-56405-6

Belli, L. (2021b). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. *The African Journal of Information and Communication (AJIC*), *28*, 1–14. https://doi.org/10.23962/10539/32208

Belli, L. (2022). Structural power as a critical element of social media platforms' private sovereignty. In E. Celeste, A. Heldt & C. Iglesias Keller (Eds.), *Constitutionalising social media*. Hart. https://doi.org/10.5040/9781509953738.ch-006

Belli, L. (2023a). Building good digital sovereignty through digital public infrastructures and digital commons in India and Brazil. G20's Think20 (T20). https://doi.org/10.2139/ssrn.4966348

Belli, L. (2023b). Exploring the key AI sovereignty enablers (KASE) of Brazil, towards an AI sovereignty stack. Pre-print version. In Carnegie Endowment for International Peace (Eds.), *Digital Democracy Network Conference 2023 essay collection*. Buenos Aires. https://cyberbrics.info/wp-content/uploads/2023/05/AI-sovereignty.pdf

Belli, L. (2023c). Exploring the key AI sovereignty enablers (KASE) of Brazil, to build an AI sovereignty stack. In L. Belli & W. B. Gaspar (Eds.), *The quest for AI sovereignty, transparency and accountability*. Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition. Fundação Getulio Vargas (FGV). https://doi.org/10.2139/ssrn.4465501

Belli, L. (2023d). To get its AI foothold, Brazil needs to apply the key AI sovereignty enablers (KASE). In S. Feldstein (Ed.), *New digital dilemmas: Resisting autocrats, navigating geopolitics, confronting platforms*. Carnegie Endowment for International Peace. https://doi.org/10.2139/ssrn.4465501

Belli, L., Franqueira, B., Bakonyi, E., Chen, L. Couto, N., Chang, S. da Hora, N., & Gaspar, W.B. (2023). *Cibersegurança: Uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano*. Fundação Getulio Vargas (FGV).

Belli, L., & Galdino de Magalhães, L. (2024). Editorial: Toward a BRICS stack? Leveraging digital transformation to construct digital sovereignty in the BRICS countries. *Computer Law & Security Review*, 55, 106064. https://doi.org/10.1016/j.clsr.2024.106064

Benyera, E. (2021). *The fourth industrial revolution and the recolonisation of Africa: The coloniality of data*. Routledge. https://doi.org/10.4324/9781003157731

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

Jiang, M., & Belli, L. (Eds). (2024). *Digital sovereignty from the BRICS countries: How the Global South and emerging power alliances are reshaping digital governance*. Cambridge University Press.

Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review, 113*(2), 501-549. https://doi.org/10.2307/1342331

Lessig, L. (2006). *Code: And other laws of cyberspace, version 2.0*. Basic Books.

O'Neill J. (2001). *Building better global economic BRICs*. Global Economics Paper No. 66. Goldman Sachs. https://www.goldmansachs.com/insights/archive/archive-pdfs/build-better-brics.pdf

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

UN General Assembly. (2024). Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on its reconvened concluding session. A/78/986-A/AC.291/28, 19 August). https://documents.un.org/doc/undoc/gen/v24/056/75/pdf/v2405675.pdf