

Geopolitics and the pursuit of informational sovereignty on the Brazil-China axis¹

Gilberto Scofield Jr.²

Universidade Federal Fluminense - UFF

Abstract:

This extended abstract examines the pursuit of digital sovereignty as a central pillar of contemporary geopolitics along the Brazil-China axis. While China employs "composite sovereignty," asserting state authority over infrastructure and data to preserve regime stability and project global power, Brazil displays structural vulnerabilities rooted in infrastructure deficits and a reliance on foreign platforms. Through bibliographic and documentary analysis, this research contrasts the Chinese model of "authoritarian informationalism" with Brazil's digital subordination. The study concludes that technology constitutes a power architecture in which China consolidates technical autonomy, whereas Brazil pursues regulatory frameworks to mitigate dependence on neo-imperialist infrastructures.

Keywords: Digital sovereignty; national security; China; regulation.

Introduction and theoretical framework

Faced with challenges such as mass disinformation and polarizing hate speech—compounded by the fact that data travels and is analyzed more easily than physical goods—the debate on digital sovereignty has become a central axis of 21st-century geopolitics (Liu, 2021). This scenario contrasts with the emergence of the internet in the 1990s, a time when “cyberspace was hailed as a borderless, decentralized and open world of free flow of information” (Wang, 2020, p. 396). In China, this sovereignty is understood as the application of State authority over infrastructure, data, and content within its virtual borders (Jiang, 2024). Theoretically, Tai and Zhu (2022) define this approach as composite sovereignty, a discursive strategy that links specific areas of Chinese development to the umbrella concept of sovereignty to legitimize regulatory intervention. Jiang (2010) uses the expression “Authoritarian Informationalism” (p. 71) to describe the same phenomenon: the use of information technologies and the internet to centralize control, monitor the population, and shape public discourse, with few openings for democratic demonstrations. Unlike the

¹ Paper presented at the 2nd Brazil-China Colloquium on Communication Sciences, a constituent event of the 49th Brazilian Congress of Communication Sciences.

² PhD student in the Graduate Program in Media and Everyday Life (PPGMC) at the Institute of Art and Social Communication, Fluminense Federal University (IACS-UFF), email: gilberto_sj@id.uff.br

utopia of a borderless global network, the Chinese model advocates for State authority over the Chinese internet as the sole legitimate decision-maker, rejecting both foreign interference and the multi-sectoral model that allows for the participation of civil society and private companies (Creemers, 2020).

In the Brazilian context, the reality of regulatory anarchy—from the perspective of both *Big Techs* platforms and artificial intelligence tools—and the lack of investments in data infrastructure limits the concept of informational sovereignty. This concept translates into the capacity to formulate public policies that guarantee State management over the production, circulation, and storage of information and data generated within its territory or by its citizens (Lastres et al., 2025). Brazil's vulnerability arises from the pervasive platformization of its society, defined by Poell, Nieborg, and Van Dijck (2019) as the deep penetration of infrastructures and algorithmic logics of digital platforms into multiple aspects of the country's social and economic life, and the cartelization of these platforms in regimes of extraction, monitoring, and sale of Brazilians' data, defined as platform capitalism (Srnicek, 2017) or surveillance capitalism (Zuboff, 2021).

Methodology and AI usage

This abstract, developed within a larger ongoing research project for an academic article, begins with a literature review that allowed for the solid theoretical construction of China's digital and data sovereignty model, as well as the position of Brazilian vulnerability. The documentary corpus includes Chinese regulatory guidelines, especially the legal framework relating to cybersecurity (China, 2016), data security (China, 2021a), and data protection (China, 2021b) created by the Chinese government. This research adopts a transparent and innovative approach by utilizing the NotebookLM platform (powered by the Gemini AI model) strictly for organizational and technical assistance, as checking references and citations according to ABNT. While these tools were employed to streamline the management of bibliographic references, facilitate the translation of primary Chinese legal sources, and assist in spelling and structural reviews, it is essential to underscore that the selection of the documentary corpus, the critical comparative analysis, and the overall intellectual synthesis were performed exclusively by the author. All AI-generated outputs, particularly regarding the interpretation of regulatory frameworks, underwent rigorous human oversight to ensure accuracy and eliminate potential hallucinations. Thus, the core scholarly

findings and the original thesis remain the sole product of human inquiry and analytical judgment.

Digital sovereignty in China: history and concepts

The Chinese trajectory in managing the digital environment can be divided into stages that reflect a transition from a concern with physical infrastructure—cables, satellites, towers, programs, data centers—to total control of the data ecosystem (Wang, 2020). Initially, starting in the 1980s, the state focus resided in the construction of the physical network and the security of information systems, with telecommunications strictly dominated by state-owned enterprises such as China Mobile, China Telecom, and China Unicom (Jiang, 2024).

The Chinese conception of cyber sovereignty was originally introduced in a 2010 Chinese manifesto on the subject, titled 'The Internet in China' (China, 2010) and published by the State Council Information Office. The white paper conceptualizes internet sovereignty in China by establishing that, “within Chinese territory, the internet is under the jurisdiction of Chinese sovereignty” (n.p.). With commercial expansion and the emergence of giants like Baidu, Alibaba, and Tencent, the country entered an era of more sophisticated content regulation, expanding the concept of sovereignty to an automatic alignment with the determinations of the government and the Communist Party of China (CPC), always focusing on internal social stability and the maintenance of the regime (Liu, 2026).

Under the administration of Xi Jinping, which began in 2013, digital sovereignty became the "cornerstone" (Creemers, 2020, p. 6) of Chinese diplomacy and domestic policy. The creation of the Cyberspace Administration of China (CAC) centralized governance, integrating national security, innovation in artificial intelligence (AI) (Hung, 2025), and the conceptualization of data as essential factors of production, comparable to land, labor, capital, and technology. This theoretical construction was followed by “China’s 2020 New Infrastructure campaign, which focuses on strengthening digital infrastructures such as 5G networks, data centers, and AI” (Liu, 2021, p. 49).

Cong (2025) observes that the concept of a "Community of Shared Future in Cyberspace," based in turn on a 2019 speech by President Xi Jinping, is the central policy guiding Chinese diplomacy in the external scenario regarding digital sovereignty. The theoretical construction proposes a global order where state sovereignty is mutually

respected, condemning Western cyber hegemony (China, 2025). In statements by government members, at world internet forums (such as Wuzhen), and in its white papers, China presents this policy under a mantle of UN-centered multilateral cooperation—not US imperialist policy in particular, or Western policies in general—security against cybercrimes, and digital inclusion for Global South countries without their own infrastructure. From this perspective, Shen (2025) argues that the free and unregulated model advocated by the US acts as an ideological facade to sustain the monopoly and surveillance power of US corporations. He further argues that the power asymmetry in the global internet architecture is the main factor sustaining this US hegemony over network governance, with the banning of TikTok in the country being a clear example of this.

Academics such as Cong (2025), Creemers (2020), and Jiang (2010) ponder that the rhetoric of democratizing international relations in the digital field serves to attract countries, especially from the Global South, that are dissatisfied with the monopoly of US Big Techs. Eder, Arcesati, and Mardell (2019) report in a Mercator Institute for China Studies (MERICS) report that China uses digital infrastructure as a proactive tool of geopolitical power through the Belt and Road Initiative (Digital Silk Road) (China, 2023). By investing billions of dollars in fiber optic cables, satellites, and data centers in developing countries, Beijing exports not only its technology but also its regulatory frameworks and surveillance systems—a strategy that challenges Western technical hegemony and promotes the idea that accelerated economic development does not depend on the adoption of liberal values of an open internet.

The State of Digital Sovereignty in Brazil

The parallel between Brazil and China reveals convergences in contesting the prevailing digital order, but profound divergences in regulatory solutions. Silveira and Xiong (2025) create a digital sovereignty index and classify Brazil at a "weak" level. None of the key indicators analyzed—which include levels of independence in data ownership and location, digital infrastructure, governance, and digital capacity—reached the level considered technical competence. The authors observe that data storage and flow remain in an initial stage of autonomy, with an almost absolute dependence on foreign providers for processing domestic information. Furthermore, the State's digital capacity is limited by low patent production and a chronic difficulty in retaining qualified talent in national universities.

This situation makes technological self-determination impossible and links the future of Brazilian development to tools that fall entirely outside its productive domain (Silveira; Xiong, 2025).

The fragility of the Brazilian digital sector is a direct reflection of the neoliberal advance observed since the 1990s, according to Silveira and Xiong. The absence of robust development policies prevented the consolidation of an independent infrastructure, resulting in an initial level of sovereignty for basic software and essential operating systems. Although there have been legislative advances such as the General Data Protection Law (LGPD) (Brasil, 2018) and the Brazilian Civil Rights Framework for the Internet (Brasil, 2014), the authors warn that governance over artificial intelligence and *Big Techs* platforms remains insufficient to ensure the integrity of public debate and the social fabric itself.

Martins and Guimarães (2026) offer, in turn, a detailed analysis of market concentration, characterizing the Brazilian digital economy as strongly subordinated to international interests. Through the lens of the Political Economy of Data and Communication, the study identifies a phenomenon in which large technology companies exercise simultaneous control over basic infrastructure and the circulation of content, crushing local competition in sectors such as cloud computing and search tools. With Google holding more than 94% of the search engine market and the Meta group dominating social networks, the country faces a rigid oligopolistic ecosystem that generates political and cultural dependence and keeps the country under the dominance of a cartel of US corporations and under the neo-imperialist whims of the Donald Trump administration (Martins; Guimarães, 2026).

Contributions and final considerations

The research demonstrates that digital sovereignty has evolved from technical protection associated with the circulation, management, and storage of personal data to a strategic resource of geopolitical and territorial power. It thus seeks to show that technology is not politically neutral, but a programmable architecture that organizes power relations and directly influences public perception and debate. Both Brazil and China view data as vital resources for development, but the ways of ensuring digital autonomy differ.

Capri (2020) analyzes how technology has become the primary battlefield of geopolitical and ideological rivalry between the United States and China, marking the end of

the era of unrestricted digital globalization and the beginning of what he conceptualizes as technonationalism. The American boycott of chip exports to China, combined with a strategy of tariff retaliations in defense of US Big Tech businesses, was met with massive investments from the Beijing government and strong direction from Chinese technology companies, state-owned or otherwise. Emerging technologies, such as artificial intelligence, 5G broadband, semiconductors, and quantum computing, have ceased to be just commercial assets and are now treated as critical tools for national security, sovereignty, and power projection. While internationally recognized brands like Alibaba, Tencent, Bytedance, and DeepSeek, among others, operate in the large Chinese retail market of startups and *Big Techs* platforms, the base of the infrastructure is concentrated in Huawei in partnership with Baidu (in the development of machine learning) and with the Semiconductor Manufacturing International Corporation (SMIC) in chip production (Chang; Arcesati; Hmaidi, 2025).

Brazil, in turn, seeks paths for democratic regulation—which has remained elusive to date—that can confront the rentierism of foreign techno-media and AI platforms, mainly from the US, and protect the public sphere from neo-imperialist policies. Faced with numerous internal and external pressures against regulation, Silveira and Xiong (2025) suggest massive investments in industrial engineering and the establishment of strategic state-owned companies capable of coordinating digital technology with a sovereign project of national development. While China consolidates a model of sovereignty that uses technology to reinforce state authority, Brazil faces the challenge of building its own regulatory frameworks to help minimize dependence on foreign infrastructures.

References

BRASIL. Presidência da República. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 9 out 2021.

BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 6 jan 2020.

CAPRI, A. Techno-nationalism: The US-China tech innovation race New challenges for markets, business and academia. [S. l.] **Hinrich Foundation**, ago 2020. Disponível em: <https://s3.iois.me/Hinrich-Foundation-Techno-nationalism-and-the-US-China-tech-innovation-race-August-2020.pdf>. Acesso em: 20 mar 2026.

CHANG, W.; ARCESATI, R.; HMAIDI, A. **China's drive toward self-reliance: Artificial intelligence chips and large language models**. Berlim: MERICS, 2025. Disponível em: <https://merics.org/en/report/chinas-drive-toward-self-reliance-artificial-intelligence-chips-large-language-models>. Acesso em: 18 mar 2026.

CHINA. Ministry of Foreign Affairs. **Building a Community with a Shared Future For Mankind**. Texto de Wang Yi. Pequim: FMPRC, 27 jan. 2025. Disponível em: https://www.fmprc.gov.cn/eng/wjbxhd/202501/t20250127_11546599.html. Acesso em: 16 mar 2025.

CHINA. National People's Congress. **Cybersecurity Law of the People's Republic of China**. Weber.cloud China, 2016. Disponível em: https://service.weber.digital/wes-uploads/Cybersecurity_Law_of_the_Peoples_Republic_of_China.pdf. Acesso em 15 mar 2025.

CHINA. National People's Congress. **Data Security Law of the People's Republic of China**. Pequim: Supreme People's Procuratorate, 10 jun 2021a. Disponível em: https://en.spp.gov.cn/2021-06/10/c_948426_2.htm. Acesso em: 15 mar 2025.

CHINA. National People's Congress. **Personal Information Protection Law of the People's Republic of China**. Pequim: NPC, 29 dec 2021b. Disponível em: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm. Acesso em: 15 mar 2025.

CHINA. State Council Information Office. **The Internet in China**. Beijing, 2010. Disponível em: http://www.china.org.cn/government/whitepaper/node_7093508.htm. Acesso em: 13 maio 2024.

CHINA. State Council Information Office. **The Belt and Road Initiative: A Key Pillar of the Global Community of Shared Future**. [S. l.]: Belt and Road Portal, 2023. Disponível em: <https://eng.yidaiyilu.gov.cn/p/86739.html>. Acesso em: 17 mar 2025.

CONG, W. The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics. In: JIANG, M.; BELLI, L. (eds.). **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance**. Cambridge, UK: Cambridge University Press, 2025. p. 63-80. Disponível em: <https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/spatial-expansion-of-chinas-digital-sovereignty/D18D59288E33063AF1EBAF416FACD6A2>. Acesso em: 16 mar 2025.

CREEMERS, R. China's Approach to Cyber Sovereignty. Berlin: **Konrad-Adenauer-Stiftung**, 2020. Disponível em: <https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty>. Acesso em: 22 jul 2022.

EDER, T.; ARCESATI, R.; MARDELL, J. Networking the "Belt and Road": The future of China's Digital Silk Road. Berlin: **MERICS**, 2019. Disponível em: <https://merics.org/en/tracker/networking-belt-and-road-future-digital>. Acesso em: 16 mar 2025.

HUNG, H. T. Exploring China's cyber sovereignty concept and artificial intelligence governance model: a machine learning approach. **Journal of Computational Social Science**, v. 8, n. 24, 2025. Disponível em: <https://link.springer.com/article/10.1007/s42001-024-00346-8>. Acesso em 17 jan 2026.

JIANG, M. Models of State Digital Sovereignty from the Global South: Diverging Experiences from China, India and South Africa. **Policy & Internet**, v. 16, p. 727-738, 15 dez 2024. Disponível em: <https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.427>. Acesso em: 12 jul 2025.

JIANG, M. Authoritarian Informationalism: China's Approach to Internet Sovereignty. **SAIS Review of International Affairs**, v. 30, n. 2, p. 71–89, 3 nov 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1702128. Acesso em: 28 set 2021.

LASTRES, H. M. M.; CASSIOLATO, J. E.; DANTAS, M. (org.). **Economia política de dados e soberania digital: conceitos, desafios e experiências no mundo**. Avaré, SP: Editora Contracorrente; Rio de Janeiro: Centro Internacional Celso Furtado, 2025.

LIU, L. The Rise of Data Politics: Digital China and the World. **Studies in Comparative International Development**, v. 56, p. 45-67, 2021. Disponível em: <https://link.springer.com/article/10.1007/s12116-021-09319-8>. Acesso em: 17 dez 2022.

LIU, R. Clustered governance: how Chinese social media platforms curate and control influencers' content creation. **Information, Communication & Society**, 12 maio 2026. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/1369118X.2026.2670738>. Acesso em 25 maio 2026.

MARTINS, H.; GUIMARÃES, J.P. **A governança econômica das plataformas digitais no Brasil**: relatório 5 do projeto “A governança econômica das redes digitais: para uma análise dos mercados e da concorrência da internet e seus impactos sobre os direitos dos usuários”. Projeto Obscom-Plataformas, Universidade Federal de Sergipe (UFS), Aracaju, 2026. 107 p. Disponível em: <https://obscomplataformas.com.br/projeto-obscom-plataformas-lanca-relatorio-sobre-economia-politica-das-plataformas-digitais-e-regulacao-no-brasil>. Acesso em: 14 maio 2026.

POELL, T.; NIEBORG, D.; VAN DIJCK, J. Platformisation. In: **Internet Policy Review: Journal on internet regulation**, v.8, n. 4, 29 nov 2019. Disponível em: <https://policyreview.info/pdf/policyreview-2019-4-1425.pdf>. Acesso em 28 set 2024.

SHEN, Y. Cyber Sovereignty and the Governance of Global Cyberspace. **Chinese Political Science Review**, [s. l.], v. 1, n. 1, p. 81-93, 2016. Disponível em: <https://link.springer.com/article/10.1007/s41111-016-0002-6>. Acesso em: 17 mar 2025.

SILVEIRA, S.A.; XIONG J. Índice de soberania digital: o caso do Brasil. In: **Liinc em Revista**, v. 21, n. 01, e7451, jun 2025. Disponível em: <https://revista.ibict.br/liinc/article/view/7451>. Acesso em: 14 ago 2025.

SRNICEK, N. **Platform capitalism**. Cambridge: Polity Press, 2017.

TAI, K.; ZHU, Y. Y. A historical explanation of Chinese cybersovereignty. **International Relations of the Asia-Pacific**, v. 22, n. 3, p. 469–499, set 2022. Disponível em: <https://academic.oup.com/irap/article/22/3/469/6514983>. Acesso em: 14 fev 2023.

WANG, A. Cyber Sovereignty at Its Boldest: A Chinese Perspective. **The Ohio State Technology Law Journal**, v. 16, n. 2, p. 395–466, 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4779801. Acesso em: 13 nov 2022.

ZUBOFF, S. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021.