

Countering Digital Colonialism: A Policy Analysis of India and Brazil

SOUMYA PANDEY¹ AND AMBUJA K. TRIPATHY*²

¹M.A. International Relations Student and ²Professor

¹South Asian University, New Delhi (India)

²Department of Political Science, Lakshmibai College, University of Delhi, New Delhi (India)

*Corresponding Author

ABSTRACT

In the contemporary digital economy, data has emerged as a critical resource, often described as the “new oil,” reshaping global power relations. This paper examines the phenomenon of digital colonialism, wherein data extraction, platform dominance, and technological dependency replicate historical patterns of colonial resource exploitation, disproportionately affecting countries of the Global South. Situating the analysis within a postcolonial political economy framework, the study undertakes a comparative policy analysis of India and Brazil to assess how these states respond to digital colonialism while pursuing digital sovereignty. The research adopts a mixed methodological approach, combining doctrinal and policy analysis with the elementary use of quantitative data, such as government data sets, official reports, and regulatory statistics. Secondary sources include academic literature, policy documents, and reliable media reports. Primary focus of the paper is on India’s Digital Personal Data Protection (DPDP) Act, 2023 and Brazil’s Lei Geral de Proteção de Dados (LGPD) to evaluate how data protection regimes function as instruments of state agency in regulating data flows, platform governance, and citizen rights. The paper argues that while both India and Brazil operate within structural constraints imposed by global digital capitalism, their data protection frameworks reflect distinct regulatory philosophies and degrees of autonomy. By highlighting similarities and divergences in their policy responses, the study contributes to debates on digital sovereignty and demonstrates how states in the Global South navigate historical legacies of dependency to shape more equitable digital futures. The findings aim to inform policymakers and scholars engaged with comparative politics, political sociology, postcolonial studies, and digital governance.

Keywords: Digital Colonialism, Data Protection, Digital Sovereignty, Global South, Digital Personal Data Protection (DPDP) Act, General Personal Data Protection Law (LGPD)

INTRODUCTION

As we can see, the twenty-first century has witnessed an unprecedented expansion of digital technologies, transforming economies, governance systems, and social systems across the globe. The internet, artificial intelligence, cloud computing, and digital platforms have created new opportunities for innovation and connectivity enabling individuals and society to participate and contribute in the changing and interconnected world. However, the benefits of the digital transformation have not been distributed equally. Control over the digital

infrastructure, data, algorithms, and online platforms are concentrated in the hands of a small number of powerful multinational technology corporations and technologically advanced states.

This unequal distribution of the digital power has given rise to the concept of digital colonialism, a phenomenon in which digital resources are extracted, controlled, and monitored by the powerful multinational technology corporations and technologically advanced states without the consent of the state whose data and resources are controlled and monitored. Similar to colonialism in the past, digital colonialism creates a new

How to cite this Article: Pandey, Soumya and Tripathy, Ambuja K. (2026). Countering Digital Colonialism: A Policy Analysis of India and Brazil. *Internat. J. Appl. Soc. Sci.*, 13 (7 & 8) : 956-963.

dependency and reinforces existing global inequalities, particularly between the Global North and Global South. Digital colonialism is also perceived as the extraction and appropriation of human life through digital data in ways that mirror historical forms of colonial resources exploitation, concentrating power and control in the hands of a few global corporations and states (Couldry and Mejias, 2019).

In response to these challenges, many developing countries are trying to build policies that are more inclined towards digital sovereignty, which means the ability of the states to exercise control over their digital infrastructure, data governance, and technological ecosystem. Among these countries, India and Brazil have emerged as significant actors to balance participation in the global digital economy as well as to protect their citizens' rights and national interest. India's Digital Personal Data Protection Act, 2023 (DPDP) and Brazil's General Data Protection Law (Lei Geral de Proteção de Dados, 2020) (LGPD) represent important policy developments through which both countries seek to strengthen data governance and advance aspects of digital sovereignty.

This work focuses on examining how India and Brazil are attempting to counter digital colonialism with the help of their respective data protection frameworks. By conducting a comparative policy analysis of the DPDP Act and LGPD, the study explores the extent to which these legal instruments promote digital sovereignty, protecting the personal data of the citizens and challenging the unequal digital power constructors. In doing so, the research contributes to the ongoing debates on digital governance, new forms of colonialism in postcolonial societies, and the future of digital rights.

The rest of this paper is structured in the following manner: the next section reviews the literature, followed by a section describing methodology. We then present results and discussion before concluding the paper.

Literature Review

Review of literature is organized around 4 broad themes: historical analysis of digital colonialism, conceptualizing digital colonialism and other related terms, digital colonialism in the contemporary world, and region-specific analysis of digital colonialism. Each of them is discussed below.

The scholarly understanding of digital colonialism has evolved considerably over the past decades- this

indicates that there is a growing recognition that digital technologies have created global inequalities and dependencies that resemble the period of colonialism in the past. While early debates on colonialism primarily focused on territorial occupation and economic exploitation, recent scholarship argues that control over data, digital infrastructure, algorithms, and technological platforms constitute contemporary extension of colonial power relations. Nothias (2025) traces the intellectual genealogy of digital colonialism by linking it to media studies, postcolonial theory, and digital activism, while Yilmaz (2025) argues that colonial patterns have increasingly embedded within global information networks. These perspectives build upon the earlier work of Schiller (1969), who argues that the communication system functions as an instrument of imperial influence, a proposition that remains relevant in understanding present day digital power structures.

As concepts evolved, scholars shifted their attention from historical interpretations to the mechanisms through which digital colonialism operates in the contemporary world. Couldry and Mejias (2019) conceptualize data colonialism as a new social order in which human experience is continuously transformed into data for commercial extraction and accumulation. Similarly, the 3CL Foundation (2025) emphasizes that the concentration of data in the hands of a few technology corporations reproduces the historical pattern of unequal resource extraction. Menon (2023) further extends this discussion by demonstrating how algorithmic systems privilege Western datasets and knowledge systems, thereby reinforcing postcolonial inequalities. Together, these studies establish digital colonialism as a multidimensional phenomena closely linked to data governance, digital sovereignty, and digital ethics rather than merely a question of technological development.

Recent literature has further expanded the discussion by examining the relationship between artificial intelligence (AI), platform capitalism, surveillance, and global digital governance. Taylor (2023) argues that AI development has intensified data extraction and infrastructural dependence, particularly across African countries, creating a new phase of resource exploitation in the digital economy. Brevini *et al.* (2025) contend that digital colonialism is sustained not only by multinational corporations (MNCs) but also by collaborations between states and technology companies that shape data governance and cross-border information flows.

Likewise, other contemporary scholars emphasize the need for equitable digital governance frameworks capable of protecting developing countries from emerging forms of digital dependence.

The literature also reveals important regional variations in how digital colonialism is understood and addressed. In India, scholarship increasingly focuses on digital sovereignty, the Digital Personal Data Protection Act, 2023, and the need to reduce the dependence on foreign digital platforms with the help of indigenous technological development. Similarly, if we look at the case of Brazil (an emerging power and economy like India) the focus is more on the Lei Geral de Proteção de Dados, 2020 (LGPD) to protect the data of the individuals. Similar discussions on Africa in general and Nigeria specifically highlight how historical colonial experience continues to influence contemporary debates on data governance, surveillance, and privacy legislation.

Based on review of literature, an important research gap is the negligible amount of work done to analyze policies in the countries in the Global South to counter digital colonialism. Mostly literature engages with the impact of digital colonialism- adequate emphasis is not given to policy analysis or comparative analysis of policies in the Global South. There is a discussion in terms of whether there should be government measures to address digital colonialism but not in terms of specifying what kind of government measures to be adopted and how to work on them to counter digital colonialism. This research is an attempt to address the research gap as identified in the process of review of literature. With regard to the theoretical framework, this paper is broadly informed by postcolonial perspective on international political economy while critically examining digital colonialism and the policy measures to counter digital colonialism in India and Brazil as two important and original member-states of the BRICS (now BRICS Plus).

METHODOLOGY

The current study adopts a mixed-method approach, combining both qualitative and quantitative techniques to gain a comprehensive understanding of digital colonialism and policy responses in India and Brazil. The qualitative component involves a doctrinal and analytical review of secondary sources, including policy documents, legal texts, scholarly articles, and reports, to explore how government frameworks address digital colonialism and promote digital

sovereignty. The quantitative component uses elementary tools, such as descriptive tables or comparative indicators in terms of numbers and percentage, to assess the extent of digital dependency and the impact of policy measures. By integrating these methods, the research aims to provide both in-depth theoretical insights and empirical evidence, enhancing the robustness and relevance of the study for the Global South.

RESULTS AND DISCUSSION

This section discusses and analyzes various dynamics surrounding the policies- the DPDP and LGPD- and also provides the readers with the outcomes and a comparative understanding based on it. Results of the research and consequent discussion are presented under the following headings:

Historical Context of the DPDP and LGPD

The findings of this study indicate that digital colonialism represents a contemporary manifestation of historical power asymmetries, wherein control over data, digital infrastructure, algorithms, and online platforms has become a significant source of economic and political influence. This increasing dominance of multinational technological corporations has intensified concern regarding digital sovereignty, data protection, and digital independence, particularly among the countries of the Global South that mostly remain dependent on foreign digital ecosystems.

A comparative study of the historical context of the DPDP and LGPD demonstrates that both India and Brazil have acknowledged these challenges and gradually developed policy frameworks to strengthen national control over digital governance. Although both countries share democratic constitutional systems (India has a prime ministerial system and Brazil has a presidential system) and rapidly expanding digital economies, their responses to digital colonialism have evolved through distinct historical, political, and institutional trajectories.

In India, the evolution of digital governance has been closely linked to rapid digital transformation and the expansion of Digital Public Infrastructure (DPI). Initiative such as Aadhaar, Unified Payments Interface (UPI), DigiLocker, and Digital India significantly enhanced digital inclusion while simultaneously generating concerns regarding privacy, surveillance, and data protection. The landmark *Justice K.S. Puttaswamy vs The Union of*

India (2017) judgement of the Supreme Court, which recognized privacy as a fundamental right under Article 21 of the Constitution, marked a turning point in India's digital governance framework. Subsequent developments, including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, debates surrounding data localization, restrictions on several foreign digital applications, and the enactment of the Digital Personal Data Protection Act, 2023, collectively demonstrate India's evolving efforts to strengthen digital sovereignty while balancing innovation, economic development, and national security.

Brazil's trajectory reflects a different yet equally significant response to digital colonialism. Influenced by constitutional commitments to individual rights and international privacy standards, Brazil adopted the Lei Geral de Proteção de Dados (LGPD), 2020, to establish a comprehensive framework governing the collection, processing, storage, and transfer of personal data. The creation of the National Data Protection Authority (ANPD) further strengthened institutional oversight by providing an independent regulatory mechanism responsible for ensuring compliance with the legislation. Unlike India's developmental approach, Brazil's framework places greater emphasis on individual privacy, transparency, accountability, and regulatory independence, reflecting a stronger rights-based orientation influenced by the General Data Protection Regulation (GDPR) of the European Union (EU).

The findings suggest that both countries look at data as of utmost importance while their responses differ in terms of governance policies and regulatory design. India seeks to balance privacy with developmental objectives, digital innovation, and strategic autonomy, whereas Brazil prioritizes comprehensive data rights and institutional accountability. Despite these differences in their frameworks, both policies aim to promote digital sovereignty of their nations.

Comparative Analysis of the DPDP and LGPD

A comparative analysis of the Digital Personal Data Protection Act, 2023 (India) and the Lei Geral de Proteção de Dados, 2020 (Brazil) illustrates that legislative frameworks in both countries showcase a significant challenge towards digital colonialism. Although enacted within different political and institutional contexts, both laws seek to regulate the collection, processing, storage, and transfer of personal data while enhancing citizen's

rights and establishing accountability mechanisms for data processing entities.

One of the principal findings of the study is that both legislations recognize personal data as an important national asset requiring legal protection. Both frameworks (the DPDP and LGPD) are built upon common principles including lawful processing, informed consent, transparency, accountability, purpose limitation, and protection against misuse of personal information. By introducing legal obligations for organizations handling personal data, both policies seek to reduce unregulated data extraction by multinational technology corporations and strengthen national control over digital governance.

However, the analysis demonstrates significant differences in their institutional approaches. Brazil's LGPD provides a comprehensive right-based framework that guarantees individuals a broad range of rights including access to personal data, correction of inaccurate information, deletion of unnecessary data, portability, and the right to revoke consent. These rights are supported by the National Data Protection Authority (ANPD), which functions as an independent regulatory institution responsible for monitoring compliance, investigating violations, and imposing sanctions where necessary.

India's DPDP Act similarly recognizes the rights of Data Principals while imposing obligations upon Data Fiduciaries to process personal information responsibly. The Act establishes mechanisms for consent-based processing, grievance redressal, and correction and erasure of personal data. Further, it introduces the Data Protection Board of India as the primary enforcement authority. At the same time, the Indian framework provides broader exemptions for governmental agencies under specified conditions relating to national security, public order, and other legitimate state functions. This reflects India's broader policy objective of balancing privacy protection with developmental priorities, governance efficiency, and digital innovation.

The findings also reveal notable differences regarding cross-border data governance. Brazil's LGPD adopts a more structured approach by regulating international data transfers through adequacy requirements and recognized safeguards that are broadly aligned with international privacy standards. And India's DPDP Act adopts a comparatively flexible framework permitting cross-border transfers except jurisdictions specifically restricted by the Central Government. This reflects India's efforts to facilitate international digital

trade while retaining regulatory discretion over sensitive data flows.

Another important observation concerns institutional capacity. Brazil's independent regulatory authority enhances transparency and regulatory accountability through specialized oversight mechanisms. In contrast, India's Data Protection Board primarily functions as an adjudicatory body constituted by the Central Government, leading to continuing academic debates regarding institutional independence and long-term regulatory effectiveness. Nevertheless, both countries recognize that effective enforcement mechanisms remain central to strengthening digital governance and ensuring compliance with data protection obligations.

From the perspective of digital colonialism, both the DPDP and LGPD contribute towards limiting unchecked data extraction and increasing national regulatory authority over digital platforms. However, the analysis also demonstrates that legal regulation alone cannot entirely eliminate structural dependence on foreign technological ecosystems. Global technology companies continue to dominate cloud infrastructure, artificial intelligence (AI) digital platforms, and digital marketplaces, thereby limiting the practical scope of legal sovereignty over data.

Comparative Analysis of the DPDP and LGPD with the General Data Protection Regulation (GDPR)

India's DPDP, Brazil's LGPD and the EU's GDPR share a common goal of safeguarding privacy, but they differ significantly in their material scope. The DPDP is uniquely restricted to digital personal data, applying only to the data collected in the digital form or non-digital data that is subsequently digitized. In contrast, the GDPR and LGPD are better and broader, applying to the processing of the personal data regardless of the means, which encompasses both the physical filing system as well as

digital records. All three frameworks maintain extraterritoriality, extending their reach to any entity outside their borders if they offer the goods or services within the respective territory.

Regarding the lawfulness of processing, all three regimes require consent to be free, informed, and unambiguous. However, while the GDPR and LGPD allow for processing based on the broad legitimate interests of the controller, provided that they do not override the individual's rights, the DPDP does not include such a general clause. Instead, the DPDP lists specific legitimate uses such as medical emergencies, employment purposes, and fulfillment of state functions like subsidies or certificates. Furthermore, the DPDP uniquely imposes statutory duties on the individuals (Data Principals) such as the duty not to file false grievances- a concept not present in the GDPR or LGPD.

The enforcement mechanisms and penalties also represent distinct regulatory philosophies. The GDPR uses a decentralized system of independent authorities with penalties reaching up to 4% of total worldwide annual turnover while ANPD can impose penalties up to 2% of an entity's revenue in Brazil (capped at R\$50 million per infraction). India's DPBI is designed as a digital office and uses a schedule of fixed-sum penalties with the highest penalty reaching Rs. 250 crore for failing to take reasonable security safeguards to prevent a data breach. While all three mandate data breach notification, the DPDP requires notifying both the board and every affected individual for every breach, whereas the LGPD and GDPR generally require notification when there is a relevant risk or damage (EU Regulation 2016/679 (General Data Protection Regulation) (2016, May 4) (Official Journal of the European Union, L 119, 1–88). Table 1 shows that India's DPDP, Brazil's LGPD, and the EU's GDPR all aim to protect personal data but differ in their scope, enforcement, and penalties. The DPDP

Table 1 : Comparative Analysis of the DPDP and LGPD with the GDPR

Aspects	DPDP (India)	LGPD (Brazil)	GDPR (EU)
Scope	Digital personal data only	All personal data	All personal data
Extraterritoriality	Yes	Yes	Yes
Lawful Basis	Consent + specific grounds (no general "legitimate interests")	Consent + legitimate interests	Consent + legitimate interests
Unique Feature	Duties on individuals (Data Principals)	None	None
Enforcement	DPBI (digital office)	ANPD	National authorities + EDPB
Penalties	Fixed penalties up to Rs. 250 crore	2% revenue, max R\$50m	4% global turnover / €20m
Breach Notification	Notify board + all affected individuals	Notify if risk/damage relevant	Notify authority in 72h; individuals if high risk

focuses mainly on digital personal data and gives duties to individuals, while the LGPD and GDPR cover broader personal data and recognize legitimate interests as a lawful basis. All three have extraterritorial reach, enforcement authorities, and breach-notification requirements, but the GDPR generally has the strongest enforcement and highest penalties.

Implications of the DPDP and LGPD for Domestic Societies in India and Brazil as well as other Developing Countries and BRICS Members

This part of the section critically analyzes the major implications of the DPDP and LGPD for the domestic society in India and Brazil respectively as well as for other developing countries and the BRICS member-states.

Implications of the DPDP for Indian society

The findings indicate that the DPDP Act, 2023 is an important step towards strengthening digital sovereignty by regulating personal data and increasing accountability among Data Fiduciaries. India's selective approach to cross-broader data transfers allows it to remain connected with the global digital economy while retaining control over sensitive digital concerns. However, stronger institutional independence, effective enforcement, and continued investment in indigenous digital infrastructure are necessary to reduce dependence on foreign technological ecosystems.

Implications of the LGPD for Brazilian society

In Brazil, the LGPD has strengthened individual data rights and established a more organized regulatory framework through the ANPD. Its rights-based approach and alignment with international data protection standards enhance accountability and facilitate Brazil's participation in the global digital economy. However, continued dependence on foreign technological platforms remains a challenge. Therefore, Brazil must complement its legal framework with greater investment in domestic technological capacity and digital infrastructure to strengthen its digital sovereignty.

Implications of the DPDP and the LGPD for other Developing Countries

India's Digital Personal Data Protection Act of 2023 eliminated most statutory barriers to cross-broader data movement, allowing transfer to any country unless the

government expressly restricts them. At the same time, Section 16(2) of the Act preserves sector-specific localization mandates for bodies such as the Reserve Bank of India (RBI), Security and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI), the Ministry of Consumer Affairs, and the Department of Telecommunication that can still require certain forms of data to be stored in India.

The DPDP's selective localization curtails the United States panopticon effect for criminal investigation and national-security purposes because data required for investigations must remain in the country, while the broader data-flow market is open to foreign firms. By keeping the flow of data largely unrestricted, India avoids a full-scale chokepoint effect, yet it leverages its regulatory autonomy to limit extraterritorial American access. Brazil's LGPD has dropped explicit data-localization requirements and instead affirms Brazil's extraterritorial reach over data concerning Brazilian citizens, granting the right to deem foreign jurisdictions "adequate" for transfers. The LGPD mirrors the EU's GDPR and represents a compromise that leaves the chokepoint effect of American dominance largely untouched, offering limited enforcement power to curb foreign access. Together, these regimes signal to other states that data-protection policies can be calibrated to protect security and domestic interests without fully closing markets. Multinational tech firms must now negotiate data-hosting arrangements that respect sectoral localization in India while complying with Brazil's broader adequacy framework, thereby reshaping global data-flow architectures and moderating, but not eliminating, American weaponized interdependence in the digital sphere (Doshi and Delgado, 2024).

Implications of the DPDP and LGPD for the BRICS Members

For the BRICS member-states, the Indian model offers a template for balancing openness with targeted sovereignty, encouraging other BRICS members to craft sector-specific localization rules that protect the sensitive data without deterring foreign investment. The DPDP's sectoral mandates also generate domestic market opportunities: Indian firms can develop data-centres and compliance services to meet regulator-imposed storage requirements, stimulating a nascent digital-infrastructure industry that can be exported to follow the BRICS economies seeking similar autonomy. At the same time,

the policy signals to multinational platforms that India will retain jurisdiction over strategic data, prompting them to negotiate data-hosting arrangements that respect local regulations. This approach other BRICS countries can leverage in bargaining with the American tech giants (Doshi and Delgado, 2024).

Brazil's LGPD, by contrast, forgoes explicit localizations and instead affirms Brazil's extraterritorial reach over personal data, adopting a GDPR-style adequacy framework. This compromise lowers compliance for foreign firms and keeps the Brazilian digital market highly integrated with the global services, benefitting BRICS partners that rely on seamless cross-broader data exchange for trade and finance. However, the LGPD's limited enforcement means Brazil remains vulnerable to the American chokepoint effect, and it demonstrates a cautionary example of how a permissive regime may preserve market access but does little to curb external digital hegemony. Together the two policies illustrate divergent pathways for BRICS nations to pursue digital sovereignty. India's targeted localization strengthens domestic control and creates exportable infrastructure, while Brazil's broader openness sustains economic integration but provides weaker protection against foreign dominance (Doshi and Delgado, 2024).

What after the DPDP and LGPD?

Following the implementation of the DPDP Act and LGPD, India and Brazil have moved from establishing data protection frameworks towards strengthening their broader digital and AI governance systems. India has adopted a technology- and development-oriented approach by introducing the DPDP Rules, AI governance guidelines, institutional mechanisms, compliance-by-design practices, and the strategic use of Digital Public Infrastructure, while also seeking a greater leadership role in digital governance in the Global South. In contrast, Brazil has focused on strengthening regulatory enforcement and institutional independence through the evolution of the ANPD, enhanced oversight mechanisms, international data-transfer standards, child digital protection, and emerging biometric data regulations. These developments demonstrate that data protection laws are not the end of digital governance reforms but rather the foundation for evolving frameworks aimed at addressing AI, digital rights, and technological sovereignty. Time will tell whether both India and Brazil are able to enact the follow-up measures to their digital governance

frameworks and implement their policies in true spirit across their vast territories.

Conclusion

The study examined digital colonialism through a comparative analysis of India's Digital Personal Data Protection (DPDP) Act, 2023 and Brazil's Lei Geral de Proteção de Dados (LGPD), 2020 to understand how policy frameworks can strengthen digital sovereignty in the Global South. The findings reveal that although digital colonialism continues to shape global power relationships through data extraction, platform dominance, and technological dependence, both India and Brazil have taken several legal and policy measures to protect personal data and enhance national control over their digital ecosystems.

The comparative analysis demonstrates that while both countries share a common objective of safeguarding citizen's data and promoting digital sovereignty, they differ in their institutional approaches and regulatory mechanisms. The study further highlights that the data protection laws alone cannot fully counter digital colonialism. Achieving meaningful digital sovereignty also requires indigenous digital infrastructure, technological innovation, ethical governance, and international cooperation among developing countries.

Overall, the research concludes that the policy experiences of India and Brazil provide valuable lessons for other nations in the Global South (especially other member-states of the BRICS) seeking to establish fair, inclusive, and sovereign digital governance. As digital technologies continue to transform global politics and economics, strengthening digital sovereignty through comprehensive legal, institutional, and technological measures will remain essential for reducing digital dependence and promoting equitable participation in the digital age.

Now we would like to briefly describe the limitations of this study and indicate areas for further research. While digital colonialism is a very broad theme, the limited scope of the research compelled the authors to engage with specific aspects of digital colonialism while focusing on a policy analysis in the context of India and Brazil. Due to the time constraint, the study could not include case studies other than India and Brazil. Let us turn to the areas for further research. First, the researchers can look at the implementation of the DPDP and LGPD in a detailed manner. Effective and equitable implementation

is crucial to the policy's success. It would be interesting to see how the concerned policies are implemented and which actors (media, voluntary organizations, and community groups in addition to the governments) play the key role in the implementation process. Second, there can be research on related developments at meso level (various provinces or states) as well as micro level (districts, cities, villages, etc.) in both India and Brazil. Since both Brazil and India have an effective and strong federal set up (India has a decentralized structure and Brazil is considered a classic case of robust federalism), it is interesting to see how data protection policies work at different levels with complex intricacies. Third, we suggest inclusion of more case studies in the comparative policy analysis. What about the other developing countries (may be other members of expanded BRICS or BRICS Plus)- what are their policy responses to digital colonialism and how effective are they? Fourth, the researchers could specifically focus on the BRICS (or BRICS Plus) as an inter-governmental organization. What kind of deliberations on digital colonialism are taking place in BRICS meetings? Can there be a collective policy to ensure digital sovereignty in the BRICS similar to the EU's GDPR?

Acknowledgment

The authors would like to thank Professor Amrita Shilpi of the Political Science Department and Dr Nivedita N of the Sociology Department at Lakshmibai College, University of Delhi for their valuable suggestions.

REFERENCES

- 3CL Foundation. (2025). *Digital colonialism and the data commons*. 3CL Foundation.
- Brevini, B., Fubara-Manuel, I., Le Ludec, C., Linaa Jensen, J., Jimenez, A., and Bates, J. (2025). Critiques of data colonialism. In J. Bates and A. Jimenez (Eds.), *Dialogues in data power* (pp. 120–137). University of Westminster Press. University of Westminster, London.
- Couldry, N. and Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press. <https://doi.org/10.1515/9781503609754> (last accessed in June 2026).
- Doneda, D. and Mendes, L./ S. (2019). A profile of the new Brazilian General Data Protection Law. In L./ Belli and O./ Cavalli (Eds.), *Internet Governance and Regulations in Latin America: Analysis of infrastructure, privacy, cybersecurity and technological developments in honor of the tenth anniversary of the South School on Internet Governance*.
- Doshi, V. and Delgado, H. E. (2024). Digital statecraft of middle powers: Tech landscape and digital sovereignty in Brazil and India. In *Popular sovereignty in the digital age* (pp. 124–132). Cambridge University Press.
- European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
- Government of Brazil. (2018). *Lei No. 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD)*. Presidência da República.
- Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Ministry of Electronics and Information Technology.
- Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)*. Ministry of Law and Justice.
- Menon, S. (2023). Postcolonial differentials in algorithmic bias: Challenging digital neo-colonialism in Africa. *SCRIPTed: A Journal of Law, Technology & Society*, 20(2), 383–399.
- Ndemo, B. (2024, August 8). Addressing digital colonialism: A path to equitable data governance. UNESCO Inclusive Policy Lab.
- Nothias, T. (2025). An intellectual history of digital colonialism. *Journal of Communication*, 75(5), 385–397.
- Schiller, H. I. (1969). *Mass communications and American empire*. Beacon Press.
- Taylor, L. (2023). Artificial intelligence, digital colonialism, and the implications for Africa's future development. *Data & Policy*, 5, E25.
- Wikipedia contributors.(n.d.). Puttaswamy v. Union of India. In Wikipedia last accessed on 02.02.2026.
- Yılmaz, Ö. (2025). The origins of digital colonialism. *Ymgelem Journal*, 16, 321–344.
