INDIA AS A POST-COLONIAL DIGITAL DEVELOPMENTAL STATE: A CRITICAL ANALYSIS

Pallavi Arora & Jyotsna Manohar[*]

As the digital economy expands, the Global South faces challenges such as platform dominance, data inequality, and a persistent digital divide, all of which echo colonial-era patterns of exploitation. These challenges, while largely driven by corporate actors, are further complicated by state actions, including surveillance, censorship, and internet shutdowns, which exacerbate control over citizens in the digital realm. Scholars have analysed these dynamics through the concept of 'digital colonialism', which highlights how the digital ecosystem mirrors colonial practices of extraction, exploitation and dispossession. While much of the discourse in the Global South centers around the role of dominant tech firms, the state also plays a critical role in perpetuating these colonial dynamics, using digital tools to reinforce its power and control. This paper critically examines India's digital governance framework, presenting it as a postcolonial digital developmental state. It evaluates India's strategies for asserting digital sovereignty, including the development of digital public infrastructure, regulating dominant platforms, and experimenting with data governance policies that prioritise community rights and non-personal data sharing. These initiatives aim to counter corporate digital colonialism and bridge the digital divide. Nevertheless, tensions remain, as state-driven practices continue to reproduce colonial dynamics of control. By analysing the strengths and limitations of India's digital governance model in addressing digital colonialism from both corporate and state actors, the paper seeks to provide valuable insights for other Global South nations aiming to create a more equitable, rights-based digital ecosystem.

TABLE OF CONTENTS

[*] Pallavi Arora is a Ph.D. candidate in international economic law at the OP Jindal Global University, Sonipat. Jyotsna Manohar is an international trade lawyer, with an LL.M. in transnational law from the Kings College, London. The authors would like to thank the NUJS Law Review for their comments and editorial insights. All errors, if any, are solely attributable to the authors. The authors may be reached at parora1@jgu.edu.in and jyotsna.manohar@gmail.com.

I. INTRODUCTION

As the global digital economy proliferates, the imperative to integrate the Global South in Industry 4.0 has taken centre stage. Despite the urgency of this challenge, several factors hinder the realisation of this goal. These include the control of large platforms over critical digital infrastructure, which they leverage to dominate digital markets, data inequality and the digital divide.[1] Existing literature has analysed these issues through the analytical lens of 'digital colonialism'.[2] According to this concept, the digital ecosystem has reproduced the dynamics of colonial exploitation, marked by extraction, exploitation and dispossession, which has led to the commodification of personal data for capitalist profit and exertion of control over marginalised communities.[3]

Several developing countries such as Indonesia, Thailand, Brazil, Mexico, South Africa, among others, are experimenting with different digital governance frameworks to assert sovereignty over the digital sphere, with a view to countering the extractive practices

[1] Richard Heeks, *Digital Inequality Beyond the Digital Divide: Conceptulizing Adverse Digital Incorporation in the Global South*, Vol. 28(4), INF. TECHNOL. DEV., 688 (2022).

[2] Michael Kwet, *Digital Colonialism: US Empire and the New Imperialism in the Global South,* Vol. 60(4), RACE CL., 3 (2019).

[3] *Id*.

of large digital corporations and fostering the growth of the domestic digital industry.[4] In this context, the present paper turns the spotlight on India's strategy for digital industrialisation. We characterise India's approach as a manifestation of a postcolonial digital developmental state. As a postcolonial state, India's approach is driven by the goal of reigning in the oligopolistic control of dominant platforms over digital infrastructure, which they leverage for extractive gain. Further, using the framework of the 'new developmental state', we explore how India's policies for developing digital public infrastructure ('DPI') and deploying data generated within India to foster the growth of the domestic digital industry could serve as a model for the Global South.

While concerns about digital colonialism in the Global South stem from the disruptive role of dominant digital firms, the state as an actor can also perpetuate colonial dynamics in the digital ecosystem. State-driven digital colonialism, a prominent concern in the Global South, is rooted in practices like state surveillance, internet shutdowns and online censorship.[5] Needless to say, for India to serve as a model for countering digital colonialism, its digital governance framework must effectively address the dual risk of exploitation from both corporate actors and the state apparatus.

Given this background, this paper critically evaluates the strengths of India's digital governance framework that may serve as a potential model for the Global South as well as areas that call for reform. Part II characterises India's approach to digital sovereignty as that of a postcolonial digital developmental state, where the state actively intervenes in the digital economy to address platform dominance, data inequality and the digital divide. Part III distinguishes the three limbs of India's approach to digital industrialisation. The *first* limb relates to the provision of DPI, focusing on infrastructure based on open networks and protocols, which India has pioneered. The *second* limb focuses on measures for reclaiming infrastructural control over digital markets from platforms through competition policy and by creating open digital infrastructure as an alternative to existing platforms. The *third* limb looks at India's data governance framework, focusing on India's proposed policy to share non-personal data ('NPD') based on the notion of community data and data trusts, as well as elements of India's trust framework. Part IV explores India's paradoxical role in navigating digital colonialism, addressing both corporate monopolies and state-driven practices like surveillance, censorship, and internet shutdowns. It underscores the importance of strengthening India's legal frameworks to better balance the twin objectives of fostering digital development and respecting individual rights and freedoms. Finally, Part V concludes.

II. DIGITAL SOVEREIGNTY IN THE GLOBAL SOUTH: REFLECTIONS ON INDIA'S JOURNEY AS A POST-COLONIAL DIGITAL DEVELOPMENTAL STATE

While the internet transcends national boundaries, the assertion of sovereign control over the digital sphere continues, resulting in various manifestations of digital sovereignty across different countries.[6] Broadly speaking, digital sovereignty refers to the ability of a state to assert authority over the digital domain within its borders,[7] including control over the

[4] Christopher Foster & Shamel Azmeh, *Latecomer Economies and National Digital Policy: An Industrial Policy Perspective*, Vol. 56(7), J. DEV. STUD., 1247 (2020).

[5] Margaret Hu, *From the National Surveillance State to the Cybersurveillance State*, Vol. 13(1), ANNU. REV. LAW SOC. SCI., 161 (2017).

[6] Anupam Chander & Haochen Sun, DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE (Oxford University Press, 2023).

[7] *Id*.

physical layer (internet infrastructure), the code layer (domain names, internet standards, and regulations) and the data layer (data itself).[8] Simply put, digital sovereignty encompasses a whole range of digital governance approaches concerning aspects such as data, cybersecurity, content moderation and the regulation of digital platforms.

So far, three dominant models for regulating the digital ecosystem—popularly referred to by Bradford as 'digital empires'—have emerged.[9] The *first* is the American market-driven model, which is centred on a free-market approach, allowing private enterprises to drive digital innovation with minimal government intervention.[10] This has led to the rise of tech giants such as Google, Apple, Meta, Amazon, and Microsoft, whose influence extends across the globe. By fostering an environment of deregulation, the United States ('US') has positioned itself as the leader in technological advancements, particularly in artificial intelligence ('AI'), cloud computing, and social media.[11] However, this model has been criticised for enabling monopolistic behaviour, data privacy breaches, and misinformation.[12] The dominance of American firms has also raised concerns over digital colonialism, as developing economies increasingly rely on US-based platforms without having much say in their governance.[13] The *second* is the European rights-driven regulatory model, which prioritises digital consumer protections, data privacy, and competition regulation.[14] The European Union ('EU') has introduced landmark regulations such as the General Data Protection Regulation ('GDPR'), the Digital Markets Act, and the Digital Services Act, all of which aim to safeguard individual rights while ensuring fair competition in the digital economy.[15] The EU's regulatory influence extends globally, through the phenomenon of 'the Brussels effect', as companies operating within the EU must comply with its stringent legal standards.[16] However, this approach has been criticised for creating bureaucratic hurdles that may stifle innovation, particularly for smaller firms struggling with compliance costs.[17] Some argue that excessive regulation could slow the EU's progress in emerging technologies, making it less competitive compared to the US and China.[18] The *third* model is the Chinese state-driven model, which is characterised by centralised state control, with the government playing an active role in regulating the digital economy.[19] Through mechanisms such as the 'Great Firewall' and data localisation

[8] Ke Xu, *Data Security Law: Location, Position and Institution Construction*, Vol. 3, BUS. & ECON. L. REV., 57 (2019).

[9] Anu Bradford, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (Oxford University Press, 2023); Chander & Sun, *supra* note 6.

[10] Bradford, *supra* note 9, 51–60.

[11] *Id*., 52–63.

[12] SUBCOMMITTEE ON ANTITRUST, COMMERCIAL AND ADMINISTRATIVE LAW OF THE COMMITTEE ON THE JUDICIARY, *Investigation of Competition in Digital Markets*, 8, 53, 133 (October, 2020) available at https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf (Last visited on February 10, 2025).

[13] Kwet, *supra* note 2, 3.

[14] Bradford, *supra* note 9, 123–168.

[15] *Id.*, 146–147, 153.

[16] *Id*., 369–371.

[17] *Id*., 158–161, 258.

[18] Erric Brattberg et al., *Europe and AI: Leading, Lagging Behind, or Carving Its Own Way?*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (2020), available at https://carnegieendowment.org/research/2020/07/europe-and-ai-leading-lagging-behind-or-carving-its-own-way?lang=en (Last visited on February 10, 2025); Jose Igancio Torreblanca & Giorgos Verdi, *Control-Alt-Deliver: A Digital Grand Strategy for the European Union*, EUROPEAN COUNCIL FOR FOREIGN RELATIONS (October 08, 2024) available at https://ecfr.eu/publication/control-alt-deliver-a-digital-grand-strategy-for-the-european-union/ (Last visited on February 10, 2025).

[19] Bradford, *supra* note 9, 82–122.

requirements, China restricts access to foreign platforms while promoting domestic alternatives like WeChat and Alibaba.[20] Although this model has bolstered domestic technological advancement, it has drawn criticism for mass surveillance, censorship, and the suppression of dissent.[21] Bradford highlights the intense rivalry between these models as the US, the EU and China compete to influence the global digital economy.[22]

Beyond the dominant digital empires, comprising the US, EU, and China, Chander and Sun highlight the Global South as an emerging player with a digital governance model tailored to its unique challenges and priorities.[23] According to them, a critical concern for the Global South is data colonialism—the extraction of data by foreign firms, which is then processed and repackaged into digital services and sold back to these countries.[24] This dynamic raises fears that the Global South will become mere suppliers of raw data while remaining dependent on Western or Chinese platforms for digital infrastructure and services.[25] This is evident in multiple cases across the Global South. In India, Facebook's Free Basics initiative sought to tighten the company's grip on the internet by controlling users' access to online content, raising concerns over censorship and surveillance before being banned for impeding net neutrality.[26] In Africa, Netflix is reportedly pulling subscribers away from local television services while acquiring regional content, making it harder for local media to compete.[27] Meanwhile, Uber's expansion has severely disrupted traditional taxi industries, sparking violent clashes in countries like South Africa and Kenya.[28]

Another pressing challenge is the digital divide in the Global South, which refers to the stark disparities in access to digital technologies, internet connectivity, and digital literacy between and within countries in the Global South.[29] Compounding this issue, dominant platforms exercise oligopolistic control over digital infrastructure, due to their first-mover advantage–largely attributable to their origin in wealthier economies with advanced technological ecosystems. Their early dominance enabled these firms to scale rapidly, amass vast datasets, and establish lock-in and network effects that reinforce their market power. As a result, these firms can impose restrictive business practices that disadvantage domestic digital firms, small businesses, and consumers, further entrenching their control over the digital economy.[30] In response to these challenges, many Global South countries are actively pursuing strategies to reclaim control over their digital ecosystems.[31]

---

[20] *Id*., 16, 84–86, 91–94, 176.

[21] *Id*., 91–98, 102–107, 118–120, 215.

[22] *See generally* Bradford *supra* note 9.

[23] Chander & Sun, *supra* note 6.

[24] *Id*., 245.

[25] *Id*.

[26] Michael Kwet, *Digital Colonialism is Threatening the Global South,* ALJAZEERA, March 13, 2019, available at https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south (Last visited on March 3, 2025).

[27] *Id*.

[28] *Id*.

[29] Heeks, *supra* note 1; *See generally* Massimo Ragnedda & Anna Gladkova, DIGITAL INEQUALITIES IN THE GLOBAL SOUTH (Palgrave Macmillan, 2020).

[30] INTERNATIONAL CHAMBER OF COMMERCE (ICC), *Global Report on Antitrust Enforcement in the Digital Economy*, 2023, available at https://iccwbo.org/wp-content/uploads/sites/3/2023/09/2023-ICC-Global-report-on-competition-enforcement-in-the-digital-economy-1.pdf (Last visited on February 10, 2025)

[31] Hu, *supra* note 5; Min Jiang & Luca Belli, DIGITAL SOVEREIGNTY IN THE BRICS COUNTRIES: HOW THE GLOBAL SOUTH AND EMERGING POWER ALLIANCES ARE RESHAPING DIGITAL GOVERNANCE, (Cambridge University Press, 2025).

The following discussion examines the key factors shaping the Global South's engagement with the digital economy and approach to digital governance. It then explores India's digital governance model as a case study of a post-colonial digital developmental state, offering insights into how Global South nations can address digital colonialism through the assertion of digital sovereignty.

A. FACTORS INFLUENCING THE GLOBAL SOUTH'S APPROACH TO DIGITAL GOVERNANCE

This sub-section begins by exploring how platform dominance, data inequality, and the digital divide create structural barriers that hinder the Global South's equitable participation in the digital economy. It then analyses these challenges through the lens of digital colonialism, revealing how dominant platforms entrench colonial patterns of exploitation in the digital sphere by reducing the Global South to data suppliers rather than equal stakeholders in the Fourth Industrial Revolution.

1. CONCERNS REGARDING PLATFORM DOMINANCE, DATA INEQUALITY AND THE DIGITAL DIVIDE IN THE GLOBAL SOUTH

A ubiquitous issue that countries, including those in the Global South, face regarding the regulation of digital markets is the limited number of platforms that exercise oligopolistic control over the digital infrastructure.[32] This stems from the massive investments required to create large consumer networks and carry out data analytics, which makes it difficult for new players to enter the market.[33] In addition to this, horizontal and vertical consolidation measures by platforms result in 'winner takes all' dynamics.[34] Needless to say, such dominance has facilitated efficiencies in logistics, payments, and service delivery—spurring innovation and expanding consumer access.[35] However, it has also led to concerns of platforms exploiting their oligopolistic control over digital infrastructure through restrictive business practices.[36] Notable in this regard is their dual role as both marketplace operators and competitors, which compromises platform neutrality.[37] This is because platforms have an incentive to prioritise their own products over those of the sellers they host. Platforms accomplish this by manipulating search results and user rating systems.[38] The *de facto* control of platforms over vast datasets further tilts the balance in their favour, allowing them to tailor

---

[32] Filippo Lancieri & Patricia Morita Sakowski, *Competition in Digital Markets: A Review of Expert Reports*, Vol. 26, STAN. J.L. BUS. & FIN., 65 (2021).

[33] *Id.*

[34] Angelina Fisher & Thomas Streinz, *Confronting Data Inequality*, Vol. 60(3), COLUM. J. TRANSNAT'L Law, 859 (2022); Paminder Jeet Singh, *Digital Industrialisation in Developing Countries - A Review of the Business and Policy Landscape,* IT FOR CHANGE, December 2017, available at https://itforchange.net/index.php/digital-industrialisation-developing-countries-%E2%80%94-a-review-of-business-and-policy-landscape (Last visited on December 23, 2024).

[35] *Id*.

[36] Dhwani Goel, *The Global Digital Divide Is Reminiscent of Colonialism*, LSE, May 6, 2021, available at https://blogs.lse.ac.uk/brexit/2021/05/06/the-global-digital-divide-is-reminiscent-of-colonialism/ (Last visited on December 23, 2024).

[37] COMPETITION COMMISSION OF INDIA, *Market Study on E-Commerce in India Key Findings and Observations*, 20 (January, 2020) available at https://www.cci.gov.in/economics-research/market-studies/details/18/6 (Last visited on December 23, 2024) ('Market Study on E-Commerce').

[38] *Id*., 21.

products and services to consumer preferences.[39] Linked to this issue is the provision of deep discounts by platforms in the e-commerce sector, which enables platforms to outprice small businesses and drive them out of the market.[40] Equally problematic is the asymmetry in contracts between platforms and business users, resulting in unfair terms that disadvantage smaller businesses.[41]

In developing countries, anti-competitive practices by digital platforms are a growing concern, as seen in several regulatory decisions.[42] In Egypt, the competition authority found that a food ordering and delivery platform abused its dominant position through exclusive dealing and tying practices, creating barriers to entry for new competitors and forcing restaurants to use its delivery service.[43] In Mexico, the competition authority blocked Walmart's acquisition of Cornershop, citing concerns that the merger would reduce competition by enabling Walmart to discriminate against its competitors on the platform and use consumer data to gain an unfair advantage.[44] Similarly, in Turkey, the competition authority ruled that Google abused its dominance in online shopping comparison services by manipulating algorithms and positioning ads in a misleading manner.[45] In India, the competition commission identified various competition-distorting practices in the e-commerce sector, such as self-preferencing, deep discounts, tying and bundling, and imposing unfair trading conditions on smaller retailers.[46] These cases highlight how digital platforms in the Global South leverage their market power to suppress competition, create entry barriers, and disadvantage local businesses, further entrenching their dominance.

Related to the issue of platform dominance is 'data inequality'. According to Fischer and Streinz, 'data inequality' refers to the situation where dominant platforms exercise control over data generation, access, and usage, which they leverage to monopolise insights on market conditions and consumer behaviour.[47] By contrast, other entities, especially in the Global South, face barriers to accessing these vast data infrastructures.[48] The legal protection of datasets through copyright and trade secrets further entrenches this inequality, stifling innovation and deepening dependency on large tech corporations. This limits the full realisation of the social and economic potential of data by hindering innovation and the development of

---

[39] Thomas Streinz, *Designing International Economic Data Law*, SSRN (2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4079058 (Last visited on December 23, 2024).

[40] Lina M. Khan, *Amazon's Antitrust Paradox,* Vol. 126, YALE L. J., 710 (2016), available at https://www.yalelawjournal.org/pdf/e.710.Khan.805_zuvfyyeh.pdf (Last visited on February 13, 2025).

[41] Market Study on E-Commerce, *supra* note 37, 30.

[42] United Nations Conference on Trade and Development, *Enforcing Competition Law in Digital Markets and Ecosystems: Policy Challenges and Options: Note by the UNCTAD Secretariat*, U.N. Doc., TD/B/C.I/CLP/74, (April 24, 2024).

[43] *Id*., 4; Amr A Abbas et al., *Egypt: New Merger Control Regime Updates Competition Law Framework*, GLOBAL COMPETITION REVIEW, June 30, 2023, available at https://globalcompetitionreview.com/review/the-european-middle-east-and-african-antitrust-review/2024/article/egypt-new-merger-control-regime-updates-competition-law-framework (Last visited on February 13, 2025).

[44] COMISIÓN FEDERAL DE COMPETENCIA ECONÓMICA, *COFECE blocked Walmart/Cornershop Concentration*, COFECE-032-2019, available at https://www.cofece.mx/wp-content/uploads/2019/06/COFECE-032-2019-English.pdf (Last visited on March 17, 2025).

[45] REKABET KURUMU, *Investigation about Alphabet Inc., Google LLC, Google International LLC, Google Ireland Limited and Google*, 7 July 2023, available at https://www.rekabet.gov.tr/en/Guncel/investigation-about-alphabet-inc-google--21d473e9b31cee118ec400505685da39 (Last visited on March 17, 2025).

[46] Market Study on E-Commerce, *supra* note 37.

[47] Fisher & Streinz, *supra* note 34, 831.

[48] *See generally* Linnet Taylor & Dennis Broeders, *In the Name of Development: Power, Profit and the Datafication of the Global South*, Vol. 64, GEOFORUM, 229 (2015).

new business models. Data inequality is further deepened by the high transaction cost of accessing data analytics, which is both capital and skill-intensive.[49]

The digital divide in the Global South further exacerbates these issues. Driven by inadequate digital infrastructure, particularly in rural areas, the digital divide limits internet access and connectivity.[50] For instance, according to the World Bank, in South Asia, rural communities face persistent gaps in digital connectivity despite increasing mobile penetration.[51] Further, while the share of the population in least developed countries ('LDCs') using the internet has increased from four percent in 2011 to thirty-six percent, about two-thirds of the LDC population still remains offline.[52] Data usage in LDCs also remains significantly more expensive than the rest of the world.[53] Another facet of the digital divide is the challenge faced by small businesses on account of their informal operations, restricted financing options, inadequate digital skills and high technology adoption costs. In Latin America, for example, micro and small enterprises account for the majority of businesses but rarely have the resources to integrate digital payment systems or e-commerce solutions effectively.[54] Similarly, in Southeast Asia, high costs of cloud services and software licensing prevent many start-ups from scaling their operations.[55] Together, these challenges limit economic opportunities and the potential for digital transformation and digital inclusion in the Global South.

The dominance of global digital platforms in the Global South has led to data inequality, market concentration, and a widening digital divide, limiting economic opportunities for local businesses.[56] These challenges reflect deeper structural imbalances, where foreign tech firms extract value from local data while restricting access to digital infrastructure.[57] This pattern mirrors historical economic dependencies and is increasingly analysed through the concept of digital colonialism. The following sub-section uses this analytical framework to contextualise the challenges facing the Global South's participation in the digital economy.

---

[49] Heeks, *supra* note 1.

[50] Anna Gladkova & Massimo Ragnedda, DIGITAL INEQUALITIES IN THE GLOBAL SOUTH (Springer, 2020).

[51] WORLD BANK GROUP, *South Asia's Digital Opportunity: Accelerating Growth, Transforming Lives*, 2022, available at https://openknowledge.worldbank.org/server/api/core/bitstreams/778a3dc7-9da1-5722-a128-50b6b2aa38d7/content (Last visited on February 11, 2025).

[52] INTERNATIONAL TELECOMMUNICATION UNION, *Measuring Digital Development Facts and Figures 2022*, available at https://www.itu.int/itu-d/reports/statistics/facts-figures-2022/ (Last visited on February 13, 2025).

[53] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *Least Developed Countries Suffer Digital Divide in Mobile Connectivity*, April 01, 2021, available at https://unctad.org/topic/least-developed-countries/chart-april-2021 (Last visited on February 13, 2025).

[54] Diego Herrera, *MSME Financing Instruments in Latin America and the Caribbean During COVID-19*, INTER-AMERICAN DEVELOPMENT BANK, May 2020, available at https://publications.iadb.org/en/msme-financing-instruments-in-latin-america-and-the-caribbean-during-covid-19 (Last visited on February 11, 2025); World Economic Forum, *Accelerating Digital Payments in Latin America and the Caribbean*, May 2022, available at https://www3.weforum.org/docs/WEF_Accelerating_Digital_Payments_in_Latin_America_and_the_Caribbean_2022.pdf (Last visited on February 11, 2025).

[55] Kenneth Tan, *Southeast Asian Companies are Massively Overpaying for Cloud Services: Why, and What Can be Done About it?*, TN GLOBAL, December 18, 2023, available at https://technode.global/2023/12/18/southeast-asian-companies-are-massively-overpaying-for-cloud-services-why-and-what-can-be-done-about-it/ (Last visited on February 11, 2025).

[56] United Nations, *Widening Digital Gap Between Developed, Developing States Threatening to Exclude World's Poorest from Next Industrial Revolution, Speakers Tell Second Committee,* U.N. Doc. GA/EF/3587 (October 06, 2023).

[57] *Id*.

2. UNDERSTANDING THE CONCERNS OF THE GLOBAL SOUTH THROUGH THE LENS OF DIGITAL COLONIALISM

In mainstream accounts, 'digital colonialism' captures the concerns of historically colonised nations about the commodification of their data by major technology firms.[58] Essentially, digital colonialism highlights the disparity where countries in the Global South possess vast amounts of unprocessed data but lack the digital infrastructure necessary to harness its full potential. This situation leads to fears of the Global South being relegated to the role of mere data suppliers, with large tech corporations extracting value from local data without equitable returns.[59] A relevant analogy can be drawn from India's handloom sector during the British Raj, where raw cotton was exported to textile mills in Manchester, only to be re-imported as finished products, thereby enriching the British East India Company at the expense of local artisans.

Beyond popular narratives, the concept of digital colonialism has received significant scholarly attention. A seminal contribution by Couldry and Mejias introduces the concept of 'data relations,' which aligns with the previously discussed notion of 'data inequality,' to define digital colonialism.[60] They describe how personal data is extracted and used within capitalist systems, making corporations and governments act as data 'colonisers'.[61] These entities control key digital infrastructures like cloud computing, search engines, social media, digital payments, e-commerce, and AI analytics.[62] Control over these digital infrastructures enables them to extract data and shape user behaviour through algorithmic targeting based on the accumulated datasets. For instance, Facebook's targeted advertising and data breaches, such as the Facebook-Cambridge Analytica scandal, have been criticised for leveraging user data to manipulate political discourse,[63] while Amazon's dominance in e-commerce allows it to prioritise its own products over those of third-party sellers, undermining local businesses.[64] This control facilitates the commodification of data and the exertion of various forms of control, including mass surveillance and restrictive business practices. Consequently, data sovereignty is undermined as individuals and nations—particularly in the Global South—often lack the means to benefit from or resist these exploitative structures.[65]

Clarke's conceptualisation of digital colonialism closely aligns with Couldry and Mejias's notion of 'data relations'. Clarke builds on their work by breaking digital colonialism into three key elements—extraction, exploitation, and dispossession—each

---

[58] Kwet, *supra* note 13.

[59] *Id.*

[60] Nick Couldry & Ulises A. Mejias, *Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject,* Vol. 20, Television& News Media 336-349 (2018).

[61] *Id.*

[62] Yuri Demchenko, Paola Grosso, Cees de Laat & Peter Membrey, *Addressing Big Data Issues in Scientific Data Infrastructure*, in *Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS)*, 48-55 (IEEE, 2013).

[63] Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach,* THE GUARDIAN, March 17, 2018, available at https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (Last visited on March 3, 2025).

[64]Khan, *supra* note 40.

[65] HARVARD LAW REVIEW, *Data Colonialism and Data Sets*, June 22, 2023, available at https://harvardlawreview.org/blog/2023/06/data-colonialism-and-data-sets/ (Last visited on February 11, 2025) ('Data Colonialism and Data Sets').

reflecting the mechanisms of 'data relations'.[66] According to Clarke, 'extraction' refers to the process of data appropriation, where corporations and governments monetise user data without meaningful consent.[67] This is evident in Google's collection of location data from Android users, even when location services are disabled, raising concerns about privacy violations.[68] 'Exploitation' reflects the structural inequalities in digital ecosystems, where dominant actors maintain control over digital infrastructures, systematically disadvantaging less powerful entities.[69] For instance, ride-hailing apps like Uber and Bolt have disrupted traditional taxi industries in countries like South Africa and Kenya, commodifying labour and profiteering at the expense of gig economy workers.[70] And 'dispossession' encapsulates the loss of autonomy and economic agency due to the monopolisation of data and digital services by tech giants, deepening dependencies on digital infrastructures controlled by them.[71] In sum, as large platforms dominate sectors such as e-commerce, ride-hailing, digital payments, and cloud computing, domestic businesses and governments in the Global South become increasingly reliant on external systems, thereby, reinforcing long-term technological subordination.[72] Together, these elements illustrate how digital colonialism extends historical patterns of extraction, exploitation and dispossession, with data serving as the new frontier of resource exploitation.

Expanding on this framework, Gray critiques the tendency to reduce digital colonialism to a mere process of extraction, rather than emphasising its deeper entrenchment in evolving orders of knowledge and value'.[73] 'Orders of knowledge', according to Gray, refer to how datafication reshapes epistemic systems by prioritising certain forms of knowledge — typically those aligned with capitalist and colonial imperatives — while marginalising indigenous and non-Western knowledge systems.[74] On the other hand, 'orders of value' pertain to how data practices assign worth to individuals, often reinforcing racialised hierarchies by exploiting specific populations disproportionately.[75] Gray posits that the interplay between 'orders of knowledge' and 'orders of value' results in 'racialised dispossession' in the digital sphere.[76] This is reflected in developments around facial recognition technology, where AI systems have been found to exhibit racial biases, disproportionately misidentifying individuals with darker skin tones.[77] These biases have resulted in wrongful arrests and increased surveillance of racialised communities.[78] Gray's argument is also illustrated in the gig

---

[66] Kayla Victoria Destiny Clarke, AMENDING AMENDMENTS: DIGITAL COLONIALISM, BILL C-11, AND ASSESSING THE CALL FOR IMPROVEMENT, 12–13 (M.A., University of Windsor, 2023).

[67] *Id*.

[68] Keith Collins, *Google Collects Android Users' Locations Even When Location Services are Disabled,* QUARTZ, November 21, 2017, available at https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled (Last visited on March 3, 2025).

[69] *Id*.

[70] Mohammad Amir Anwar, Elly Otieno & Malte Stein, *Locked In, Logged Out: Pandemic and Ride-Hailing in South Africa and Kenya,* Vol. 60(4) J. MOD. AFR. STUD. (2022).

[71] *Id*.

[72] Data Colonialism and Data Sets, *supra* note 65.

[73] Catorina Gray, *More than Extraction: Rethinking Data's Colonial Political Economy*, Vol. 17(2), INT. POLITICAL SOCIOL., 13–14 (2023).

[74] *Id*., 3.

[75] *Id*.

[76] Gray, *supra* note 73, 3, 12, 16.

[77] U.N. Human Rights Council, *Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, Ashwini K.P.*, U.N. Doc. A/HRC/56/68 (June 3, 2024).

[78] Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.*, MIT TECHNOLOGY REVIEW, July 17, 2020, available at

economy, where platforms, such as Amazon and Uber, often exploit workers through algorithmic wage suppression and precarious employment conditions, mirroring dynamics of colonial labour exploitation.[79] Here, 'orders of value' operate through algorithmic wage suppression, where workers in the gig economy are assigned lower economic worth.[80] By treating gig economy workers as entities to be optimised for cost-efficiency rather than recognising their agency or lived realities, these platforms reinforce historical patterns of labour exploitation.

In sum, digital colonialism describes an unequal global order where dominant technology firms and states extract, monetise, and control key digital resources and infrastructure, thereby, reinforcing economic and racialised inequalities in the digital sphere. Against this backdrop, the next section explores India's approach to digital governance, assessing its response to digital colonialism and its potential as a model for the Global South.

B. INDIA'S APPROACH TO DIGITAL INDUSTRIALISATION: A POSTCOLONIAL DIGITAL DEVELOPMENTAL STATE

As a postcolonial state, India's approach to digital industrialisation is driven by a nationalist vision that seeks to assert digital sovereignty in response to the threat of digital colonialism by Big Tech.[81] In line with Clarke's understanding of digital colonialism, India's digital governance framework targets the 'extraction', 'exploitation' and 'dispossession' of data belonging to Indian citizens by foreign corporations without equitable returns to the domestic digital industry.[82] In response to these concerns, India has espoused a 'data for development' approach.[83] Such an approach challenges the asymmetrical power dynamics of data relations by ensuring that data-driven economic benefits are distributed more equitably within India, rather than being monopolised by dominant tech giants. Pursuant to this, India treats the data generated within its borders as a public good to foster digital innovation and strengthen its domestic digital industry. In addition, India poses an epistemic challenge to the US-led model of international digital trade rules at the World Trade Organisation, which advocates for unrestricted cross-border data flows.[84] In India's view, developing countries require policy flexibility to craft data governance frameworks tailored to their unique

---

https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ (Last visited on February 12, 2025).

[79] Ruchi Singh & Vani Bhushan, *The Global Workforce Revolution: Exploring Digital Labour Platforms and the Gig Economy in the Era of Globalization*, Vol. 3(2), INT. J. CIV. LAW LEGAL RES., 19-27 (2023)

[80] Wena Teng, *Paid by AI: Algorithmic Wage Discrimination in the Gig Economy,* COLUMBIA UNDERGRADUATE LAW REVIEW (2025), available at https://www.culawreview.org/journal/paid-by-ai-algorithmic-wage-discrimination-in-the-gig-economy#:~:text=Given%20the%20decentralized%20nature%20of,ongoing%20exploitation%20through%20unfair%2C%20deceptive (Last visited on March 3, 2025).

[81] Neha Mishra, *Data Governance and Digital Trade in India: Losing Sight of the Forest for the Trees?* in DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE (Anupam Chander & Haochen Sun eds,, Oxford University Press, 2023).

[82] *Id*., 3; MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, *Strategy for National Open Digital Ecosystems (NODE)*, *Consultation Whitepaper*, available at https://ourgovdotin.wordpress.com/wp-content/uploads/2020/02/mygov_158219311451553221.pdf (Last visited on December 23, 2024).

[83] Draft National Data Governance Framework Policy, 2022, Preamble, ¶1.1.

[84] Sunday Guardian, *India's Concerns Validated as US Withdraws Support for Some WTO E-Commerce Proposals*, 29 October 2024, available at https://sundayguardianlive.com/top-five/indias-concerns-validated-as-us-withdraws-support-for-some-wto-e-commerce-proposals (Last visited on December 23, 2024).

developmental needs.[85] This would enable them to strengthen local digital ecosystems while safeguarding against risks of data misuse and foreign surveillance.[86]

Beyond the postcolonial imperatives shaping India's digital governance stance, a notable aspect of its approach is the state's interventionist role in the digital economy. India's strategy for digital industrialisation is rooted in a mixed economy model, where the state plays a central role alongside private players to ensure the growth of the domestic digital sector.[87] The government positions itself as a key market player, spearheading the development of DPI, fostering domestic innovation, and ensuring the growth of the local digital sector.

The central role played by the state in India's digital economy can be likened to that of the developmental state. This model of economic development is typically associated with the East Asian tiger economies of the twentieth century.[88] The key features of the developmental state are strong state intervention in the economy, economic planning, and collaboration with the private sector.[89] It particularly emphasises import substitution policies to protect domestic industries and limit reliance on international markets. However, following the Washington Consensus, the rise of neoliberal ideas marked a shift towards deregulation, privatisation and market liberalisation.[90]

Nevertheless, in recent years, we have witnessed a backlash against neoliberal ideals. This has given ascendence to the idea of what Trubek calls the 'new developmental state', a progressive approach to economic development that builds on traditional developmentalism but adapts to the global economy.[91] The model stresses the importance of both the state and the private sector in shaping economic outcomes, recognising that neither can succeed alone.[92] Instead of direct state control, industrial policies focus on fostering public-private partnerships and guiding private-sector activities. The approach also advocates for flexible industrial policies grounded in a high degree of experimentation and adaptability.[93]

India's approach to digital industrialisation has the characteristics of the new developmental state. Under the Indian model, state intervention in the digital economy serves three primary objectives.[94] *Firstly*, it aims to build robust DPI to bridge the digital divide.

---

[85] Rahul Matthan et al., *Data Governance, Asian Alternatives: How India and Korea are Creating New Models and Policies*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, August 2022 available at https://carnegie-production-assets.s3.amazonaws.com/static/files/Data_Governance_v1.pdf (Last visited on December 20, 2024).

[86] *Id*.

[87] Mishra, *supra* note 81, 3, 14.

[88] Ipek Danju et al., *The East Asian Model of Economic Development and Developing Countries*, PROCEDIA – SOCIAL AND BEHAVIORAL SCIENCES (2014), available at https://www.researchgate.net/publication/273851728_The_East_Asian_Model_of_Economic_Development_and_Developing_Countries (Last visited on December 23, 2024).

[89] Meredith Woo-Cummings, THE DEVELOPMENTAL STATE, (Cornell University Press, 1999); Niraj Kumar, *Democratic Development State in India*, Vol. 62(2), INDIAN J. OF PUB. ADMIN., 226 (2017).

[90] David M. Trubek, *Developmental States and the Legal Order: Towards a New Political Economy of Development and Law* 1–2, 5 (Univ. of Wisconsin Legal Studies Research Paper No. 1075, 2008) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1349163 (Last visited on December 21, 2024).

[91] *Id*.

[92] *Id*., 8.

[93] *Id*., 9, 10; Dani Rodrik & Ricardo Hausmann, *Doomed to Choose: Industrial Policy as Predicament*, September 2, 2006, HARVARD UNIVERSITY available at https://drodrik.scholar.harvard.edu/publications/doomed-choose-industrial-policy-predicament (Last visited on December 21, 2024).

[94] IT FOR CHANGE, *Digital Industrialisation in Developing Countries: A Review of the Business and Policy Landscape*, December 2017, available at https://itforchange.net/sites/default/files/1468/Digital-industrialisation-May-2018.pdf (Last visited on February 10, 2025).

Secondly, it seeks to combat the increasing dominance of major platforms by reclaiming infrastructural control over digital markets. *Thirdly*, it aims to redistribute control over data to stimulate innovation and create new commercial opportunities for the domestic digital industry. Through this approach, India seeks to foster a vibrant digital ecosystem, creating opportunities for domestic digital firms, especially indigenous data-driven start-ups and small businesses, creating national champions or home-grown alternates to foreign tech giants, fostering innovation and new business models, as well as levelling the playing field.[95] By taking an active market role, the Indian state positions itself not just as a regulator but as a key driver of economic transformation, aligning with the principles of the new developmental state.

India's strategies to combat digital colonialism mainly target large digital corporations, but the Global South also faces threats from state practices that mirror colonial exploitation and control.[96] These practices include state surveillance, internet shutdowns, and online censorship, which have led to concerns about state-driven digital colonialism.[97] In India, the Constitution serves as a bulwark against state overreach. In fact, the constitutionality of India's legislative framework — spanning data privacy, online censorship, and internet shutdowns — has, on many an occasion, been scrutinised by the Supreme Court.[98] However, commentators emphasise the need for reforms and stronger procedural safeguards to better balance individual autonomy with developmental imperatives and foster trust in the Indian digital ecosystem.[99]

In sum, India's digital industrialisation strategy seeks to counter digital colonialism by reclaiming data control, fostering domestic innovation, and strengthening its digital economy. Through a 'data for development' approach and state-led interventions, India challenges foreign tech dominance while promoting equitable access to digital resources. However, concerns over surveillance, censorship, and internet restrictions highlight tensions between state control and individual rights. A truly equitable digital future requires balancing digital sovereignty with robust safeguards for privacy, freedom of expression, and democratic accountability.

Given this background, Part III of the paper explores India's legislative and policy initiatives as a postcolonial digital developmental state aimed at curbing the dominance of large platforms and creating a level playing field in the digital ecosystem, offering a potential model for the Global South. Thereafter, Part IV elaborates on how the state's assertion of sovereignty over the digital ecosystem could reproduce colonial dynamics of exploitation, and using this framing analyses the legal framework governing state surveillance, internet shutdowns and censorship in India.

---

[95] *Id*.

[96] Mihir Kaulgud, *India's Approach to Data Decolonization: Moving Away from the "Data as Resource" Metaphor*, SOCIAL AND POLITICAL RESEARCH FOUNDATION, October 2022, available at https://sprf.in/wp-content/uploads/2022/10/data-decol-IB.pdf (Last visited on December 23, 2024).

[97] Hu, *supra* note 5; Chander & Sun, *supra* note 6.

[98] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 ('Puttaswamy'); Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 ('Anuradha Bhasin'); Shreya Singhal v. Union of India, (2015) 5 SCC 1 ('Shreya Singhal').

[99] Mishra, *supra* note 81; Amoha Basrur et al., *The Digital Personal Data Protection Act, 2023: Recommendations for Inclusion in the Digital India Act*, OBSERVER RESEARCH FOUNDATION, October 30, 2023, available at https://www.orfonline.org/research/the-digital-personal-data-protection-act-2023-recommendations-for-inclusion-in-the-digital-india-act (Last visited on December 23, 2024); VIDHI CENTRE FOR LEGAL POLICY, *Comments on the Draft Digital Personal Data Protection Bill, 2022*, December 2022, available at https://vidhilegalpolicy.in/wp-content/uploads/2023/01/221221_DPDPB-Comments_Vidhi_Final.docx.pdf (Last visited on December 23, 2024).

III. KEY ELEMENTS OF INDIA'S DIGITAL INDUSTRIALISATION APPROACH AS A PARADIGM FOR THE GLOBAL SOUTH

India's digital industrialisation strategy can broadly be classified into three limbs. The *first* limb relates to developing DPI to close the digital divide and leverage digitalisation for national development. The *second* limb aims to counter the growing influence of major platforms by reclaiming infrastructural control over digital markets. The *third* limb focuses on redistributing control over data for developmental purposes. This Part critically analyses India's digital policies under the above three limbs that may serve as a model for digital development in the Global South.

A. DEVELOPING DIGITAL PUBLIC INFRASTRUCTURE THROUGH INDIA STACK

The G20 New Delhi Leader's Declaration of 2023 underscores the crucial role of DPI established on open standards and underpinned by open-source software.[100] In line with this vision, India is one of the pioneers in implementing DPI based on a series of open protocol frameworks, layered on top of one another, called India Stack.[101] At the foundation of India Stack lies the infrastructure concerning digital identity called Aadhaar, the world's largest biometric national identification system. Built on top of the Aadhaar system, in a digital stack, are open protocol infrastructure and standards for digital payment, consented data sharing and unbundled commerce.

1. THE AADHAAR DIGITAL IDENTITY PROGRAMME

The Aadhaar program was introduced to provide Indian residents with a unique identity number based on their biometric and demographic data.[102] In 2017, the Indian Supreme Court upheld the constitutionality of the Aadhaar Act by ruling that it did not violate the fundamental right to privacy of Indian citizens or create a surveillance state.[103] The Court also held that the requirement to provide Aadhaar details to access government welfare schemes or file taxes was constitutionally valid. However, the court disallowed private entities from mandatorily seeking Aadhaar information for digital authentication purposes. Subsequently, the Aadhaar Act was amended to give effect to the judgment.[104]

Aadhaar has played a significant role in bridging the digital divide in India. It is estimated that Aadhar has contributed $15.1 billion to India's GDP in 2022.[105] Today, Aadhar provides a digital ID to over 1.38 billion Indian residents, or approximately ninety-seven percent of the population.[106] Notably, Aadhaar's coverage in twenty-six states/union territories

---

[100] MINISTRY OF EXTERNAL AFFAIRS, *G20 New Delhi Leader's Declaration* September 9, 2023, available at https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf (Last visited on December 20, 2024) ('G20 New Delhi Leaders Declaration').

[101] INDIA STACK, *India Stack*, available at https://indiastack.org/index.html (Last visited December 20, 2024).

[102] UNIQUE IDENTIFICATION AUTHORITY OF INDIA, *Vision & Mission*, available at https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india/vision-mission.html (Last visited on December 20, 2024).

[103] Puttaswamy, *supra* note 98.

[104] The Aadhaar and Other Laws (Amendment) Act, 2019.

[105] NASSCOM, *India's Digital Public Infrastructure: Accelerating India's Digital Inclusion,* February 2024, available at https://community.nasscom.in/sites/default/files/publicreport/Digital%20Public%20Infrastructure%2022-2-2024_compressed.pdf (Last visited on February 11, 2025) ('NASSCOM Report'), 41.

[106] Press Release, MINISTRY OF ELECTRONICS & IT, *Government of India Taking Measures to Enhance the Reach of Indian Digital Public Infrastructure*, July 26, 2024, available at https://pib.gov.in/PressReleseDetailm.aspx?PRID=2037598&reg=3&lang=1 (Last visisted on March 17, 2025).

has reached saturation levels of more than ninety percent while six states/union territories have coverage between eighty to ninety percent.[107] This has reduced transaction costs and enabled access to government schemes, subsidies, better credit options, and priority in procurement.[108] Aadhaar-based digital authentication has also lowered the cost of onboarding entities to the banking system, thereby promoting financial inclusion.[109] For instance, the population gaining access to bank accounts under the Jan Dhan Yojna has risen from forty-four percent in 2016 to seventy-seven percent in 2023.[110] Additionally, it has helped individuals and businesses secure mobile and internet connections, accelerating their digitalisation.[111]

Despite these advancements, the Aadhaar program has faced significant criticism, particularly concerning privacy and data security. In October 2023, a massive data breach exposed the personal information of approximately 815 million Indian citizens, including Aadhaar and passport details, which were reportedly put up for sale on the dark web.[112] In response, India enacted the Digital Personal Data Protection Act ('DPDP') in 2023, modelled on the EU GDPR, to strengthen data security and privacy safeguards. However, the Act has sparked concerns over state-driven digital colonialism due to broad exemptions that allow government agencies extensive access to personal data—an issue examined in greater detail in Part IV.A.

2. Digital Payments: Unified Payments Interface

The next layer of India Stack, known as the Unified Payments Interface ('UPI'), aims to make digital transactions cheaper and more accessible. UPI is India's largest payment network, with approximately USD 127 billion worth of transactions in 2022.[113] Given its success in India, UPI has been introduced in France, the United Arab Emirates, Bhutan, Singapore, Nepal, Sri Lanka and Mauritius.[114]

India's UPI system is unique in that it operates on an open-source API and is structured as a three-level stack. The base layer is operated by the National Payments Corporation of India, the second layer includes regulated financial entities like banks, and the top layer comprises payment applications operated by fintech players. UPI's interoperability allows every participant in the payment stack to interact with others using the same universal set of APIs, eliminating the need to establish one-to-one relationships between banks to transfer money.[115]

UPI has driven digitalisation in India by reducing reliance on cash and enabling seamless, low-cost, real-time financial transactions. In January, 2025 alone, nearly seventeen

---

[107] NASSCOM Report, *supra* note 105.

[108] The World Bank Group, *G20 Digital Identity Onboarding*, 2018, available at https://documents1.worldbank.org/curated/en/362991536649062411/pdf/129861WP-10-9-2018-17-26-21-GDigitalIdentityOnboardingReportlowres.pdf (Last visited on December 21, 2024).

[109] The World Bank Group, *Private Sector Economic Impacts from Identification Systems*, 2018, available at https://www.worldbank.org/en/publication/globalfindex/Report (Last visited on December 21, 2024).

[110] NASSCOM Report, *supra* note 105, 43.

[111] Matthan et al., *supra* note 85.

[112] Debanjan Sadhya & Tanya Sahu, *A Critical Survey of the Security and Privacy Aspects of the Aadhaar Framework*, Vol. 140, Computers & Security (2024).

[113] National Payment Corporation of India, *Unified Payments Interface (UPI)*, available at https://www.npci.org.in/what-we-do/upi/product-overview (Last visited on December 20, 2024) ('NPCI').

[114] Naina Bhardwaj & Melissa Cyrill, *Unified Payments Interface (UPI) from India: Expanding Global Use*, India Briefing News, February 15, 2024, available at https://www.india-briefing.com/news/global-acceptance-of-india-unified-payments-interface-upi-tracker-26183.html/ (Last visited on December 20, 2024).

[115] NPCI, *supra* note 113.

billion transactions, valued at over USD 270 billion, were completed in India using UPI.[116] Its interoperability has expanded access to digital financial services across sectors and communities, fostering digital inclusion.[117] Additionally, UPI has spurred fintech innovation, cementing India's position as a leader in digital finance.[118]

3. CONSENTED DATA SHARING: DATA EMPOWERMENT AND PROTECTION ARCHITECTURE

The third layer of India Stack seeks to facilitate consented data sharing through a framework called Data Empowerment and Protection Architecture ('DEPA'), an innovative techno-legal framework for data governance. While privacy laws recognise the rights of data principals to control their data, they fall short in providing them with effective means to do so. On the other hand, DEPA grants data principals greater agency over their data by enabling them to transfer their data among different data fiduciaries.[119] Moreover, DEPA ensures the privacy of data principals by mandating that all data transfers between data fiduciaries occur *via* an encrypted digital workflow activated by obtaining the electronic consent of the data principal, managed by institutional intermediaries called consent managers.[120]

Currently, DEPA has been introduced in the financial services sector,[121] with efforts underway to extend its implementation to other domains such as telecom, healthcare, and education. By enabling seamless and secure data sharing between financial institutions, DEPA addresses longstanding challenges associated with data inaccessibility and asymmetry. This framework empowers individuals and businesses to leverage their financial data to access loans and other financial products at competitive rates, fostering greater financial inclusion.[122] Furthermore, DEPA's foundation on open protocols and standards distinguishes it from other data portability mechanisms, which are often hindered by a lack of standardisation and fragmented data storage formats.[123]

In sum, India Stack harnesses open-source frameworks like Aadhaar, UPI, and DEPA to enhance financial inclusion, lower costs, and enable secure data sharing. Building on this foundation, Part B examines India's regulatory approach to reclaiming infrastructural

---

[116] NPCI, *Monthly Metrics (2023)*, available at https://www.npci.org.in/statistics/monthly-metrics (Last visited on February 11, 2025).

[117] Yan Carriere-Swallow, Vikram Haskar & Manasa Patnam, *Stacking Up Financial Inclusion Gains in India,* INTERNATIONAL MONETARY FUND, July 2021, available at https://www.imf.org/external/pubs/ft/fandd/2021/07/india-stack-financial-access-and-digital-inclusion.htm (Last visited on February 13, 2025).

[118] Anit Mukherjee & Ashwini Joshi, *Digital Public Infrastructure as a Catalyst for Private Sector Innovation*, OBSERVER RESEARCH FOUNDATION, January 20, 2025, available at https://www.orfonline.org/research/digital-public-infrastructure-as-a-catalyst-for-private-sector-innovation (Last visited on February 13, 2025).

[119] NITI Aayog, *Data Empowerment and Protection Architecture: A Secure Consent-Based Data Sharing Framework to Accelerate Financial Inclusion,* March 2023, available at https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf (Last visited on February 10, 2025)

[120] *Id*.

[121] OECN, *Open Credit Enablement Network*, available at https://ispirt.github.io/ (Last visited December 20, 2024).

[122] Siddharth Dixit, *India's Digital Transformation Could be a Game-Changer for Economic Development*, WORLD BANK BLOGS, June 20, 2023, available at https://blogs.worldbank.org/en/developmenttalk/indias-digital-transformation-could-be-game-changer-economic-development (Last visited on December 21, 2024).

[123] Vikas Kathuria, *Data Empowerment and Protection Architecture: Concept and Assessment*, OBSERVER RESEARCH FOUNDATION, August 12, 2021 available at https://www.orfonline.org/research/data-empowerment-and-protection-architecture-concept-and-assessment (Last visited on December 21, 2024).

control over digital markets through competition policy and the development of open-network DPI.

B. RECLAIMING INFRASTRUCTURAL CONTROL OVER DIGITAL MARKETS FROM PLATFORMS

As mentioned, digital infrastructure is controlled by dominant platforms. These platforms have an oligopoly over digital markets, enabling them to adopt practices that may distort competition. To regain infrastructural control from digital platforms, India has implemented measures to regulate platforms through competition policy and by developing DPI as an alternative to platforms. The following discussion takes a closer look at innovative advances made by India to address these issues.

1. OPEN NETWORK DIGITAL INFRASTRUCTURE AS AN ALTERNATIVE TO DIGITAL PLATFORMS

India's transition from a platform-centric to an open-network model aims to address key challenges associated with platform dominance in e-commerce.[124] As discussed, currently, major platforms control access to digital markets, favouring their own products and services while limiting competition. This creates high entry barriers for small businesses, restricts consumer choice, and concentrates data in the hands of a few corporations. By shifting to an open-network model, India seeks to decentralise digital commerce, promote fair competition, and ensure broader participation by smaller players.

In this light, in 2022, India launched the Open Network for Digital Commerce ('ONDC'), the unbundled commerce feature of India Stack.[125] This tech-based initiative fosters open networks for exchanging goods and services over a digital network. The Indian government plays a crucial role in ONDC as both an enabler and regulator, ensuring it fosters competition and reduces reliance on dominant platforms like Amazon and Flipkart. Led by the Department for Promotion of Industry and Internal Trade, ONDC is part of India's broader DPI strategy to create an open, decentralised e-commerce ecosystem. The government provides policy direction, regulatory support, and financial backing through institutions like the Quality Council of India.[126] To drive adoption, it actively promotes ONDC among small businesses through incentives, workshops, and partnerships with public-sector banks. While market forces will shape ONDC's success, the state's role in infrastructure, regulation, and adoption remains essential.

To be clear, ONDC is not an application, intermediary, marketplace or software. Instead, it is a set of protocols and specifications facilitating open connection and interaction between buyers, platforms, and retailers.[127] The two key features of ONDC are interoperability

---

[124] Press Information Bureau, *Government of India Launches New Initiative to Boost Digital Economy*, April 2022, available at https://pib.gov.in/PressReleasePage.aspx?PRID=2090097 (Last visited on February 12, 2025).

[125] OPEN NETWORK FOR DIGITAL COMMERCE, *All About Open Network for Digital Commerce,* July 2022, available at http://ondc.org/about-ondc/ (Last visited on December 20, 2024).

[126] Pinki Rani & Priti Yadav, *Unlocking the Potential: A Comprehensive Analysis of ONDC*, Vol. 3(2), INT. J. CIV. L. & LEGAL RES., 19 (2023).

[127] Mahesh K.M. et al., *Open Network for Digital Commerce -ONDC (E-Commerce) Infrastructure: To Promote SME/ MSME Sector for Inclusive and Sustainable Digital Economic Growth,* Vol. 7, INT. J. MANAG. TECHNOL. SOC. SCI., 320 (2022).

and unbundling of commerce.[128] ONDC supports interoperability by allowing buyers and sellers to transact regardless of their host platform. For example, a buyer registered on Amazon may directly purchase goods from a seller listed on Flipkart. Thus, unlike the current model, where buyers and sellers must use the same platform or application, resulting in a network effect, ONDC is more decentralised, allowing buyers and sellers to transact regardless of the platforms on which they are registered. The other relevant feature of ONDC is the unbundling of commerce. Unlike platforms, which control the entire chain of services from seller onboarding to customer acquisition, delivery fulfilment, and grievance resolution, ONDC breaks this down into separate services. This enables seamless interaction between the various entities in the e-commerce ecosystem and fosters competition between relevant players.

Due to its decentralised nature, ONDC could disrupt the oligopolistic control of platforms over digital markets. In contrast to platforms that charge exorbitant commissions for hosting sellers, ONDC enables seller onboarding for free, making it possible for businesses to compete with the prices offered by other players in the digital market. Additionally, ONDC's support for interoperability makes it platform-agnostic. This helps counter the monopoly practices of platforms that disrupt the level-playing-field in e-commerce.[129]

Despite the rapid strides in developing open network DPI, the ONDC initiative is still nascent. Presently, Paytm and Snapdeal are the only major applications that have been integrated with ONDC. Meanwhile, despite integrating its logistics and analytics services, Amazon has yet to come on board with its e-commerce arm. By contrast, other major platforms, like Flipkart, have chosen not to participate in the initiative.[130] This cautious approach by major players highlights the challenges of onboarding established platforms. Observers note that established players with significant investments in their digital platform value chain might prefer to compete with ONDC rather than integrate with the network.[131] Thus, it remains to be seen how successful ONDC would be in establishing a level-playing-field in India's e-commerce sector.

2. COMPETITION POLICY

Apart from developing an open-network DPI, competition policy can also be used to regulate the infrastructural control of platforms over digital markets. Investigations into the anti-competitive conduct of platforms by the competition authorities in the EU and anti-trust authorities in the US have triggered a debate about the scope and purpose of competition law in the digital economy.[132] Despite being a relatively young regulator, India's CCI has also initiated probes into alleged anti-competitive conduct by platforms.

A fundamental requirement in competition law is the presence of an abuse of a dominant market position within the relevant market.[133] A dominant position refers to a

[128] Paridhi Puri, Bhakti Jain & Karishma Sharma, *Open Network for Digital Commerce: Revolutionising the Revolution*, INVEST INDIA, October 2021, available at https://www.investindia.gov.in/team-india-blogs/open-network-digital-commerce-revolutionising-revolution (Last visited on December 20, 2024).

[129] KINARA CAPITAL, *ONDC Accelerating the Growth of MSMEs in India*, November 2022, available at https://kinaracapital.com/open-network-for-digital-commerce-is-poised-to-accelerate-the-growth-of-msmes-in-india/ (Last visited on December 20, 2024).

[130] Varsha Meghani, *ONDC Is India's Next Big Bet After UPI*, FORBES INDIA, May 22, 2023, available at https://www.forbesindia.com/article/take-one-big-story-of-the-day/ondc-is-indias-next-big-bet-after-upi/85073/1 (Last visited on December 20, 2024).

[131] *Id*.

[132] Khan, *supra* note 40.

[133] The Competition Act, 2002, §4.

situation where an enterprise enjoys significant market power, allowing it to operate independently of competitive forces or influence market dynamics.[134] Abuse of this position occurs when a dominant entity engages in practices that restrict competition, such as predatory pricing, exclusionary conduct, or unfair contractual terms.[135]

Several high-profile cases from India include the complaint against MakeMyTrip, Goibibo, and OYO — the online travel and hospitality platforms—for resorting to platform parity clauses to prevent their hotel partners from offering lower rates than those listed on the platform.[136] These platforms have also been accused of charging exorbitant commissions, providing deep discounts, and preferentially treating certain hotels. Similarly, Flipkart has been investigated for discriminating between sellers on its platform.[137] Uber was investigated for offering deep discounts and restricting associated drivers from working with competing radio taxi operators.[138] In another instance, SnapDeal, an e-commerce platform, and SanDisk, a manufacturer of digital storage devices, have been accused of collusion to prevent the aggrieved seller from offering SanDisk products on SnapDeal.[139] Google was accused of abusing its dominance by enforcing unfair contract terms, including mandatory pre-installation of its apps and leveraging its search dominance to benefit other services.[140] Most recently, the CCI investigated WhatsApp for abusing its dominant position in the over-the-top ('OTT') messaging market to impose unfair terms on users.[141] This case marked a pivotal moment in competition law enforcement in India, as the CCI recognised privacy as a non-price parameter of competition, thus expanding the scope of its regulatory oversight to include consumer autonomy and data protection, and aligning with global trends in grappling with the dual challenge of digital dominance and privacy.[142]

It is worth noting that out of the above cases, the CCI found anti-competitive conduct only in three instances, namely, by Google, MakeMyTrip, and WhatsApp. In the remaining cases, the CCI did not observe an abuse of dominant market position by the concerned platforms. This difference in outcomes raises fundamental questions about applying competition law to digital markets. Notably, digital markets are highly complex and dynamic. Therefore, the key concepts of competition policy, like the scope of the relevant market and determination of market power, must be adapted to suit the peculiarities of digital markets.[143] Since the CCI is a comparatively young regulator, its approach to regulating digital markets is gradually evolving. In what follows, the paper delves into the unique challenges that digital

---

[134] *Id*.,

[135] *Id*. §4(2).

[136] Federation of Hotel & Restaurant Associations of India (FHRAI) v. MakeMyTrip (MMT), Case No. 14/2019 and 01/2020, Competition Commission of India ('MakeMyTrip').

[137] All India Online Vendors Association v. Flipkart India Pvt Ltd, Case No. 20/2018, Competition Commission of India.

[138] Meru Travel Solutions Pvt. Ltd. (MTSPL) v. Uber India Systems Pvt. Ltd., Case No. 25/2017, 27/2017 and 28/2017, Competition Commission of India.

[139] Ashish Ahuja v. SanDisk Corp, Case No. 17/2014, Competition Commission of India ('SanDisk').

[140] Umar Javeed v. Google LLC, Case No. 39/2018, Competition Commission of India ('Google LLC').

[141] In re: Updated Terms of Service and Privacy Policy for WhatsApp Users, Case No. 01/2021 with In re: Prachi Kohli v. WhatsApp LLC, Case No. 05/2021 with In re: Internet Freedom Foundation v. WhatsApp LLC, Case No. 30/2021, Competition Commission of India ('WhatsApp LLC').

[142] K.R. Srivats, *WhatsApp Case: CCI Restores User Sovereignty, Privacy Declared a Key Parameter of Competition*, THE HINDU BUSINESS LINE, November 20, 2024, available at https://www.thehindubusinessline.com/companies/whatsapp-case-cci-restores-user-sovereignty-privacy-declared-a-key-parameter-of-competition/article68888926.ece (Last visited on December 23, 2024).

[143] U.N. Conference on Trade and Development, *Competition Law, Policy and Regulation in the Digital Era*, ¶7, U.N. Doc. TD/B/C.I/CLP/57 (April 28, 2021).

markets present for competition law and policy and the developments in Indian law and practice to effectively counter the competition-distorting practices of platforms.

A crucial factor in an anti-competition investigation is determining the scope of the relevant market within which the alleged anti-competitive activity occurs.[144] Defining the relevant market too broadly would make it harder to establish an entity's dominant position and abuse of market power.[145] The CCI's approach to defining the relevant market in the digital sphere has gradually evolved. Initially, the CCI considered both the offline and online segments as two distribution channels of a single relevant market.[146] This broad notion of the relevant market made it challenging to establish the incidence of anti-competitive conduct. However, in subsequent cases, like the investigation into MakeMyTrip, the CCI separated the offline and online segments into two distinct relevant markets, thereby limiting the scope of the relevant market.[147] In the recent investigation against Google, the CCI identified multiple sides of the relevant market, further narrowing the scope of assessment to each side of the market so identified.[148] In the probe against WhatsApp, the CCI went even further and found that even within the online advertising market, there exists a further two kinds of markets: namely, the market for online search advertising ads (i.e. ads displayed when a user inputs a query in the search engine), and the market for online display advertising (i.e. ads displayed when a user is consuming content online).[149] This progressive narrowing of the 'relevant market' reflects a growing appreciation of the complexities of digital competition and signals an evolving regulatory framework that is more aligned with global competition trends by considering the nuances of platform-based business models.

Another key assessment in an anti-competition investigation is an entity's abuse of its dominant position in the relevant market.[150] As regards traditional markets, competition authorities have been considering an entity's market share to assess its market power. However, the unique characteristics of digital markets make this determination more complex.[151] To begin with, unlike traditional markets, digital platforms operate with a dual market structure, with one market involving the consumer and the platform and the other involving the seller and the platform.[152] The two markets are interdependent and influence each other through a network effect.[153] Consequently, an increase in the number of consumers on a platform tends to attract more sellers on the said platform and *vice-versa*. The network effect is critical in determining an entity's dominant position in digital markets. It creates a situation where consumers and sellers get locked-in on a particular platform, making it difficult for them to switch to other platforms. Unlike regulators in the EU and US that have long recognised the network effect as a factor in assessing market dominance in digital markets,[154] it is only recently

[144] Katarína Kalesná, *Relevant Market - Digital Challenges,* Vol. 7(1), BRATISL. L. REV., 77 (2023).
[145] *Id*.
[146] SanDisk, *supra* note 139, ¶16.
[147] MakeMyTrip, *supra* note 136, ¶198.
[148] Google LLC, *supra* note 140, ¶615.
[149] WhatsApp LLC, *supra* note 141, ¶10.
[150] Kalesná, *supra* note 144.
[151] OECD, *Ex Ante Regulation and Competition in Digital Markets,* 2021, available at https://web-archive.oecd.org/2021-12-01/616997-ex-ante-regulation-and-competition-in-digital-markets-2021.pdf (Last visited on December 20, 2024).
[152] OECD, *Rethinking Antitrust Tools for Multi-Sided Platforms 2018*, April 2018, available at https://www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.htm (Last visited on December 20, 2024).
[153] *Id*.
[154] Google Search (Shopping), Case AT.39740, ¶314 (European Commission); Microsoft v. Commission, Case T-201/04, ¶558 (Court of First Instance of the European Communities); United States v. Microsoft Corp., 253

that the CCI has started considering the network effect as a criterion to determine market power, as observed in the investigations against WhatsApp, Google and MakeMyTrip. [155] In addition, factors like zero-price services, multi-homing, and market tipping complicate the determination of the dominant market position in the digital sphere.[156]

Notably, in January 2020, the CCI released the Market Study on E-commerce in India: Key Findings and Observations, which identified several competition issues in the e-commerce sector.[157] The report highlighted concerns such as platform neutrality, deep discounting, exclusive agreements, and a lack of transparency in search rankings and data collection practices. The CCI emphasised the need for increased transparency to reduce information asymmetry and foster sustainable business relationships among stakeholders.[158]

In light of the evolving character of the digital economy, in 2023, the Committee on Digital Competition Law was constituted to examine the adequacy of India's competition law to regulate emergent practices in digital markets. The committee has proposed the *ex-ante* regulation of digital markets in line with the EU's Digital Markets Act.[159] Compared to competition law, which focuses on the effects of an alleged anti-competitive activity on a *post-facto* basis, *ex-ante* regulation takes a preventive approach by prohibiting specific anti-competitive practices beforehand.

The committee has recommended enacting the Digital Competition Act. It proposes the *ex-ante* regulation of entities susceptible to market concentration, called Systemically Significant Digital Enterprises ('SSDEs'), like search engines, social networking services, operating systems and web browsers.[160] The committee recommends using quantitative and qualitative thresholds to identify SSDEs. The quantitative criteria include an entity's (i) significant financial strength, based on factors like turnover, gross merchandise value, and market capitalisation, and (ii) significant spread based on the number of businesses and end users in India. The qualitative criteria include an entity's resources and volume of aggregated data. The draft bill prohibits SSDEs from engaging in practices like fair and transparent dealing,[161] self-preferencing,[162] using non-public data of business users to compete with them,[163] using or sharing users' personal data across services or with third parties without their consent,[164] restricting users from using third-party applications,[165] preventing business users from contacting customers, promoting offers, or directing them to other services, unless such restrictions are essential to its core services,[166] and tying and bundling.[167] Thus, a key

F.3d 34, 49 (United States Court of Appeals for the District of Columbia Circuit); FTC v. Meta Platforms Inc., Civil Action No. 20-3590 (JEB), 48 (United States Court of Appeals for the District of Columbia Circuit).

[155] WhatsApp LLC, *supra* note 141, ¶10; Google LLC, *supra* note 140, ¶¶155, 186–202, 283, 290–291; MakeMyTrip, *supra* note 136, ¶¶30, 194, 226, 232.

[156] Marco Iansiti, *The Value of Data and Its Impact on Competition,* (Harvard Business School, Working Paper No. 22-002, 2021).

[157] Market Study on E-Commerce, *supra* note 37, 30.

[158] *Id*.

[159] COMMITTEE ON DIGITAL COMPETITION LAW, *Report of the Committee on Digital Competition Law*, 59 (February 27, 2024).

[160] *Id*., 17.

[161] The Draft Digital Competition Bill, 2024, §10.

[162] *Id.,* §11.

[163] *Id.,* §12(1).

[164] *Id.,* §12(2).

[165] *Id.,* §13.

[166] *Id.,* §14.

[167] *Id.,* §15.

consideration before Indian regulators is whether such issues could be better addressed through *ex-ante* regulation, given that *ex-post* competition law enforcement is slower, more resource-intensive, and subject to a case-by-case assessment, making it less effective in curbing recurring anti-competitive practices in digital markets.[168]

Another crucial aspect to consider is the adequacy of competition law in addressing data inequality. In *Vinod Kumar Gupta* v. *Whatsapp Inc.*, the CCI observed that in a data-driven economy, competition law needs to examine the anti-competitive implications of data concentration by platforms.[169] However, Fisher and Streinz point out that while data concentration might enable platforms to acquire a monopoly position, it does not, of itself, pose a problem from an anti-trust law perspective unless it leads to abuse of a dominant position in the relevant market.[170] In other words, competition law focuses on preventing anti-competitive conduct based on the strict criteria of abuse of market dominance, rather than addressing broader concerns about unequal access to data or its redistribution for developmental purposes. Consequently, India has turned to its data policy to redistribute the control over data for developmental purposes. The following sub-section examines how India's data policy seeks to achieve its stated objective of 'data for development'.

C. DEVELOPMENTAL APPROACH TO DATA GOVERNANCE

A key pillar of India's digital industrialisation strategy is an experimental approach to data governance.[171] India's data policy is driven by the imperative to tackle data inequality by redistributing control over data, which is concentrated in the hands of dominant platforms. The following discussion unpacks the measures being contemplated by India to implement its vision of 'data for development'.[172]

Tackling distributive data inequality is the cornerstone of India's data governance framework. In this regard, India is exploring policies to redistribute the control over data, which is currently concentrated in the hands of dominant platforms. These policies aim to encourage innovation and new business models in India and enable small businesses to access data more easily.

1. SHARING OF OPEN GOVERNMENT DATA AND NON-PERSONAL DATA

It is widely recognised that the government enjoys a formidable position in data ecology. To harness the economic and social potential of government data, recent agreements on digital trade call for open government data, with the underlying objective of stimulating innovation and new business models, thereby creating new business opportunities.[173] In line with this vision, India has established the Open Government Data Platform to enable single-point access to data belonging to the Government of India.[174]

---

[168] *Id.*
[169] Vinod Kumar Gupta v. WhatsApp Inc., Case No. 99/2016, Competition Commission of India, ¶9.
[170] Fisher & Streinz, *supra* note 34, 829, 859.
[171] *Id*.
[172] Mishra, *supra* note 81.
[173] Mira Burri & Rodrigo Polanco, *Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset,* Vol. 23(1), J. INTL. ECON. L., 187 (2020); India-United Arab Emirates Comprehensive Economic Partnership Agreement, 2022, Art. 9.12.
[174] OPEN GOVERNMENT DATA PLATFORM INDIA, *Engagement Through Data*, available at https://data.gov.in/ (Last visited on December 20, 2024).

Apart from the open government data initiative, the Indian government is taking steps to promote the sharing of NPD collected by government entities. NPD refers to data that is unrelated to an individual, such as weather conditions or data generated from public infrastructure.[175] Additionally, it includes information that was initially personal but has been anonymised to the point where it cannot be used to identify an individual, such as anonymised healthcare records of patients. Following the recognition of privacy as a fundamental right by the Supreme Court in *K.S. Puttaswamy* v. *Union of India* ('Puttaswamy'), India has placed emphasis on safeguarding personal data.[176] At the same time, India is evaluating the proposal to regulate NPD to facilitate access to social and economic data for developmental purposes through the Draft National Data Governance Framework Policy, 2022.[177]

This policy is based on the notion of data trusts and community rights over data.[178] It is built on the premise that a community should be allowed to benefit from the NPD that pertains to it. The government has been accorded the role of a trustee to ensure that the economic benefits of NPD accrue to the concerned community. Put differently, under the policy, data is seen as an economic asset of which the government is the trustee.

The policy aims to establish the India Datasets program to share the NPD collected by government entities in India. Private organisations are also encouraged to share their NPD with the program. This is a significant departure from the previous recommendations, which proposed the mandatory sharing of NPD held by private entities.[179] The policy establishes the India Datasets platform to enable Indian entities to access these datasets. The implementation of the policy will be overseen by the Indian Data Management Office ('IDMO'), which will also evaluate requests for accessing data under the policy.[180]

One of the objectives of creating NPD datasets is to encourage innovation and develop new business models. Further, with the government's impetus to establish a data analytics ecosystem, domestic digital firms could draw inferences and gain insights from an NPD dataset, which would help them improve the quality of their products and services in line with consumer preferences. It would also enable domestic digital firms to scale their data-based businesses.

The proposed NPD sharing framework is at a preliminary stage, and commentators have pointed out certain gaps that call for greater clarity as the proposals advance into legislation.[181] One issue concerns the ineffectiveness of anonymisation techniques — methods used to remove or obscure personal identifiers from data. Research has shown that even anonymised data can sometimes be re-identified by cross-referencing it with other datasets, raising concerns about privacy and security.[182] This challenges the assumption that NPD can be neatly separated from personal data. Since policymakers often treat NPD as a

---

[175] KRIS GOPALAKRISHNAN COMMITTEE, *Report by the Committee of Experts on Non-Personal Data Governance Framework*, 13 (July 2020) ('Gopalakrishnan Committee').

[176] Puttaswamy, *supra* note 98.

[177] Draft National Data Governance Framework Policy, 2022, Preamble, ¶1.1.

[178] Consumer Unity and Trust Society (CUTS) International, *Future of Non-Personal Data Governance in India: A Consumer Perspective*, April 2021, available at https://cuts-ccier.org/pdf/policy-brief-future-of-npd-governance-in-india.pdf (Last visited on December 20, 2024) ('CUTS').

[179] Gopalakrishnan Committee, *supra* note 175, 37.

[180] CUTS, *supra* note 178.

[181] Alex Hern, *Anonymised Data Never Be Anonymous Enough, Study Finds*, THE GUARDIAN, July 23, 2019, available at https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds (Last visited on February 11, 2025).

[182] *Id.*

distinct category with fewer privacy protections, the risk of re-identification blurs this distinction, necessitating a more nuanced regulatory approach to safeguard individual privacy.[183] The proposed policy seeks to address this issue by making the IDMO responsible for prescribing protocols for the anonymisation of data and for ensuring privacy in the course of data sharing under the framework. However, how the final report of the NPD framework distinguishes between non-personal and personal data remains to be seen.[184]

Secondly, it is apprehended that large and digitally enabled firms may become disproportionate users of these datasets, as small digital firms may not have access to adequate data analytics infrastructure to draw inferences from them.[185] To address this issue, India's proposals for sharing NPD and open government data must be accompanied by efforts to strengthen the domestic data analytics and cloud computing ecosystem, enabling small businesses to effectively leverage NPD datasets by accessing cloud-based data storage, analytics and other related services.

The final issue relates to the granularity of data subject to sharing under the NPD framework. While raw data can be characterised as *res communis* — i.e., a public good that no one can own — this may not be the case for aggregated data (aggregated view of data across multiple data points) and inferred data (insights derived from data using advanced analytics).[186] Unlike raw data, aggregated and inferred data often represent a competitive advantage for businesses. From an IP perspective, refined and analysed data may form part of an entity's proprietary assets in the form of copyright and trade secrets, necessitating either due compensation or licensing mechanisms to govern its usage fairly.[187] This raises questions about how private entities who volunteer to share such data would be adequately compensated.

The regulatory challenges in governing NPD must be considered alongside India's evolving approach to data flows, particularly as the country reassesses its stance on data localisation and cross-border data transfers. This brings us to the broader debate on transnational data mobility and India's shifting position on data localisation, discussed below.

2. Transnational Data Mobility and Data Localisation

India's experimental approach to data governance is most manifest in the context of cross-border data flows and data localisation requirements. India initially viewed data generated within the country as a national resource and prescribed data localisation to utilise data for domestic digital development.[188] However, this has given way to a more open approach that seeks to balance free data flows with trust.

To be clear, data localisation refers to the practice of storing and processing data within a specific geographic boundary, typically within a country's borders.[189] This practice mandates that data generated or collected within a country be stored and managed within that country, sometimes accompanied by restrictions on its transfer to other jurisdictions. Data localisation can apply to a wide range of data, including personal information, financial

[183] *Id.*
[184] Mishra, *supra* note 81.
[185] Matthan et al., *supra* note 85.
[186] Fisher & Streinz, *supra* note 34.
[187] *Id*.
[188] Draft National e-Commerce Policy 2019, 8.
[189] Konstantinos Komaitis, *The 'wicked problem' of Data Localisation*, Vol. 2(3), J. Cyber Policy, 355 (2017).

records, and industrial data.[190] It is often driven by concerns related to national security, privacy, sovereignty, and economic competitiveness.

Countries like China and Russia have introduced various forms of data localisation, often citing similar reasons of protecting national security, data sovereignty, and ensuring consumer protection.[191] On the other hand, the EU has incorporated conditional data localisation under the GDPR by allowing cross-border data transfers as long as the receiving country provides adequate data protection safeguards.[192] However, the EU does impose restrictions on data transfers to countries that lack equivalent data protection laws, thus requiring additional safeguards such as the use of Standard Contractual Clauses or Binding Corporate Rules to ensure that personal data remains protected when transferred outside the EU.

When it comes to India, its Draft E-Commerce Policy of 2019 took a protectionist approach insofar as it sought to introduce data localisation for domestic digital development.[193] The policy proposed restrictions on the cross-border flow of data generated from Internet of Things devices, e-commerce platforms, social media and search engines.[194] By enabling domestic entities to access this data, the policy aimed to facilitate innovation and new business models, thereby creating new commercial opportunities for domestic digital firms.[195] Further, it sought to strengthen India's data centre and cloud-computing ecosystem, thus facilitating participation of domestic firms in the data economy.[196]

However, several criticisms have been levelled against data localisation as a tool for economic development. Data localisation, while aimed at enhancing data sovereignty and security, presents several significant challenges that make its implementation complex and potentially counterproductive. Economically, it imposes high costs on businesses, particularly startups and small enterprises, which rely on affordable global cloud services.[197] Mandating local data storage requires substantial investments in domestic infrastructure, driving up operational expenses and limiting access to advanced global technologies.[198] This, in turn, can stifle innovation and reduce the competitiveness of local businesses in international markets.[199]

Moreover, localisation risks isolating a country's digital ecosystem from the global flow of data, a phenomenon referred to as digital balkanisation.[200] This fragmentation undermines cross-border collaboration, a critical factor for developing data-driven technologies and ensuring efficient global services.[201] Despite its intent to enhance security, localisation often provides a false sense of protection, as cyber threats are global in nature and

---

[190] *Id*.

[191] Liliya Khasanova & Katharin Tai, *Shades of Authoritarian Digital Sovereignty: Divergences in Russian and Chinese Data Localisation Regimes*, Vol. 9(1), J. CYBER POLICY, 70 (2024).

[192] Komaitis, *supra* note 189.

[193] Draft National e-Commerce Policy 2019.

[194] Matthan et al., *supra* note 85.

[195] Arindrajit Basu et al., *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*, CENTRE FOR INTERNET AND SOCIETY, March 19, 2019, available at https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf (Last visited on December 20, 2024).

[196] *Id*.

[197] *Id*.

[198] *Id*.

[199] *Id*.

[200] Erica Fraser, *Data Localisation and the Balkanisation of the Internet,* Vol. 13(3), SCRIPTED, 359 (2016).

[201] *Id*.

require international cooperation for effective mitigation. Without robust cybersecurity measures, domestic storage alone cannot prevent breaches or misuse.[202]

These concerns, among others, prompted a new wave of policy thinking around cross-border data flows and data localisation in India. The Draft E-Commerce Policy was eventually withdrawn. Subsequently, at the G20 Summit of 2023, India expressed support for the notion of 'free data flow with trust', i.e., allowing data to move seamlessly across borders while ensuring privacy and consumer protection. [203] marking a shift from its 2019 stance at the G20 Osaka Summit, where it opposed this concept.[204]

To support this vision, India has enacted the DPDP Act, which assumes the free flow of cross-border data as the norm while allowing the government to restrict data flows to certain countries by notification.[205] The law suggests that such restrictions may be imposed if India is not satisfied with the adequacy of personal data protection in the transferee country's jurisdiction or for national security purposes.[206] The law also permits sector-specific agencies, such as the central bank, to impose localisation requirements.[207] Finally, data localisation may be imposed for law enforcement purposes.[208] Thus, while the DPDP Act advances a broader shift away from stringent data localisation in favour of supporting cross-border data flow, it acknowledges the necessity of certain restrictions, particularly in the context of national security and sectoral requirements.

Building on this framework, the introduction of the DPDP Rules in 2025 further expands the government's role in determining the parameters of data localisation. These rules grant the central government significant discretion in specifying which data should be localised, the types of data subject to localisation, and the conditions under which cross-border data transfers may occur. In particular, the Rules impose additional localisation requirements in two critical areas. Rule 14, which governs cross-border data transfers, stipulates that personal data may only be transferred outside India if it meets criteria established by the central government.[209] Rule 12(4) adds another layer, placing an obligation on Significant Data Fiduciaries to store specified personal and traffic data pertaining to its flow exclusively within India.[210] In effect, these Rules further cement the central government's broad authority over data localisation and cross-border data flow, reinforcing the state's control over the digital landscape.

In sum, India's position on data localisation has evolved from a perspective that considers data a valuable national resource to be stored locally for domestic digital development to a more market-oriented approach, subject to safeguards for privacy and regulatory purposes. However, with the introduction of the DPDP Rules, the government now holds significant discretion in determining data localisation policies and the conditions governing cross-border data flows. Additionally, India has extended the 'data for development' framing to NPD and is actively evaluating policy proposals to share such data with domestic

[202] *Id*.
[203] G20 New Delhi Leaders Declaration, *supra* note 100.
[204] Matthan et al., *supra* note 85.
[205] The Digital Personal Data Protection Act, 2023, §16.
[206] *Id*., §17(2).
[207] *Id*., §16(2).
[208] *Id*., §17(1)(c).
[209] Draft Digital Personal Data Protection Rules, 2025, R. 14.
[210] *Id*., R. 12(4).

entities to foster innovation and create new commercial opportunities for domestic digital firms.

IV. INDIA AND DIGITAL COLONIALISM: NAVIGATING PARADOXES

Part III highlighted several notable aspects of India's approach to digital industrialisation that may serve as a model for the Global South in fighting digital colonialism stemming from the pervasive control of large digital corporations over digital infrastructure and data. As discussed, these strategies aim to establish digital public infrastructure, reclaim from digital giants their entrenched control over digital infrastructure and redistribute the benefits of data for national development. These strategies, while credible from the standpoint of trying to reign in the oligopoly control of large digital firms, may not offer a holistic response to digital colonialism, as the Global South also faces the spectre of state-driven digital colonialism with rising instances of state surveillance, online censorship and internet shutdowns. These practices expose the extractive and exploitative tendencies of governments themselves.

This tension reflects the paradox of the postcolonial digital developmental state. On the one hand, the Global South positions itself as a digital developmental state by actively intervening in the digital economy to counter foreign corporate control and foster self-sufficiency. This developmentalist vision is driven by a nationalist agenda of digital sovereignty, which seeks to reclaim authority over data and digital infrastructure. However, in their pursuit of digital autonomy, states often reproduce internal colonial dynamics, effectively positioning themselves as new agents of digital colonialism. While resisting external corporate dominance, they simultaneously deploy extractive and exploitative governance strategies that mirror the very colonial logics of control they seek to dismantle.

This dynamic becomes evident in practices such as state surveillance, online censorship, and internet shutdowns, which reflect the patterns of extraction, exploitation, and dispossession that Clarke identifies as characteristic of digital colonialism.[211] However, a critical distinction lies in the fact that these practices are primarily enforced by state actors rather than by monopolistic digital corporations. This shift emphasises the role of the state in perpetuating colonial dynamics within the digital sphere. For example, through mass surveillance, the state appropriates the personal data of citizens as a means to exert control and generate profit.[212] This mirrors the concept of 'data relations' that Couldry and Mejias identify as central to digital colonialism.[213] Such commodification of personal data transforms individuals into sources of value while depriving them of meaningful control over their digital identities–a process reminiscent of colonial exploitation that undermined individual autonomy. Furthermore, by disproportionately targeting marginalised communities along ethnic, racial, caste and class lines, state surveillance reinforces racialised hierarchies associated with colonial practices that historically treated certain groups as inherently exploitable.[214] Put differently, just as colonial orders of value privileged certain groups while subjugating others, contemporary surveillance regimes reinforce existing hierarchies by subjecting specific populations to intensified monitoring and control.[215]

[211] Clarke, *supra* note 66, 12.

[212] *Id*., 166; Couldry & Mejias, *supra* note 60, 12–13.

[213] Couldry & Mejias, *supra* note 60.

[214] Gray, *supra* note 73, 3.

[215] *Id*.

Likewise, online censorship becomes a tool for suppressing dissent from marginalised groups to reinforce dominant narratives.[216] This is reminiscent of colonial suppression of local knowledge systems in favour of imposed ideological frameworks.[217] In the same vein, internet shutdowns represent an assertion of state control over digital infrastructure, whereby individuals and communities are denied not only their freedom of speech and expression but also their right to economic participation in the digital economy, thereby reproducing the dispossessory dynamics inherent in digital colonialism.[218] Further, internet shutdowns perpetuate the political suppression of various forms of social mobilisation and collective action, echoing the exploitative aspects of historical colonialism within the digital sphere.[219]

In view of the foregoing, while efforts in the Global South seek to reclaim digital sovereignty from corporate monopolies, they must also confront the risks of state-driven digital colonialism. Without robust legal safeguards, state control over digital systems risks replicating the very extractive and exploitative structures that postcolonial digital development aims to dismantle. These concerns are particularly relevant as India positions itself as a leader in shaping digital governance frameworks across the Global South. To fulfil this role effectively, India must first strengthen its own legal framework to address these challenges. The following discussion reviews India's existing legal framework on the protection of personal data, internet shutdowns, and online censorship, while drawing on existing literature to identify suggestions for reform and improvement.

A. PERSONAL DATA PROTECTION FRAMEWORK

While India's data governance regime is framed around the rhetoric of digital sovereignty, it reproduces colonial dynamics through state surveillance, data collection, and opaque decision-making, often at the expense of individual privacy. The following discussion delves deeper into India's data protection framework, highlighting how its broad exemptions and weak oversight mechanisms would likely contribute to state-driven digital colonialism.

In India, domestic and international factors have influenced the development of a comprehensive data protection framework. Domestically, the apex court's recognition of privacy as a fundamental right in the Puttaswamy case initiated the creation of a cross-sectoral data protection framework.[220] Internationally, the EU's GDPR is influencing data protection norms globally. This is because of the GDPR's extra-territorial nature, which empowers the EU to restrict the transfer of personal data to third countries failing to meet its data protection standards.[221]

In 2023, India enacted the DPDP Act to introduce a framework for cross-sectoral data protection.[222] The Act was introduced at a time when the Indian government was already facing considerable backlash for the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('IT Rules'), which disproportionately increased

---

[216] *Id*.

[217] *Id*.

[218] *Id*.; Clarke, *supra* note 66, 43.

[219] Gray, *supra* note 73, 3; Clarke, *supra* note 66, 45.

[220] Puttaswamy, *supra* note 98.

[221] Giulio Vittorio Cervi, *Why and How Does the EU Rule Global Digital Policy: An Empirical Analysis of EU Regulatory Influence in Data Protection Laws*, Vol. 1(2), DIGITAL SOCIETY, 18 (2022); Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, Vol. 71(2), FLA. L. REV, 365 (2019).

[222] The Digital Personal Data Protection Act, 2023.

government control over online content and raised privacy concerns.[223] Similar to the GDPR, the DPDP Act also has an extra-territorial application.[224] It establishes the rights of data subjects and the obligations of data fiduciaries (entities collecting or processing personal data), with penalties for non-compliance.[225]

However, the DPDP Act differs from the GDPR in certain critical aspects. *First,* the Act's scope is restricted as it does not protect non-digital personal data, opening the potential for misuse of such data.[226] In contrast, the GDPR safeguards personal data in all forms, whether digital or manual.[227] *Second,* the DPDP Act excludes personal data made publicly available, though it remains unclear if such data can be processed or only viewed.[228] *Third*, the Act lacks a classification system for sensitive personal data, unlike the GDPR, which provides extra protection for data like racial, political, or religious information.[229] The earlier 2019 version of the bill included such classifications, but these were removed.[230] *Fourth*, the DPDP Act does not impose criminal liability for breaches; instead, it only applies monetary penalties,[231] which may not be sufficient in severe cases.[232] Previous versions of the bill had included criminal offences, such as data de-anonymisation.[233] *Finally*, the Act does not establish a compensation mechanism for victims of data breaches, removing the provisions of §43A of the Information Technology Act, 2000 ('IT Act'), which previously allowed compensation for failure to protect sensitive personal data.

Scholars also highlight the presence of state carve-outs from the obligations under the DPDP Act.[234] To begin with, under §17(1)(c) of the Act, data can be processed without consent for purposes such as the prevention, detection, investigation, or prosecution of offences. §17(2)(a) goes further, granting blanket exemptions to any government agency that the government may notify, citing reasons like sovereignty, security, integrity, public order, or preventing incitement. This effectively places these agencies outside the purview of the law. Additionally, §17(2)(b) exempts the state from consent requirements for processing data for research, archival, or statistical purposes. This is supplemented by Rule 15, which exempts data processing for research, archiving, or statistics but does not clarify what qualifies as legitimate research or who can use this exemption, nor does it require consent from data principals.[235] Further, §7 of the Act, read with Rule 5, permits government instrumentalities to

---

[223] Draconian Rules: The Hindu Editorial on the Impact of the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, THE HINDU, April 10, 2023, available at https://www.thehindu.com/opinion/editorial/draconian-rules-the-hindu-editorial-on-the-impact-of-the-it-intermediary-guidelines-and-digital-media-ethics-code-amendment-rules-2023/article66717811.ece (Last visited on February 12, 2025).

[224] The Digital Personal Data Protection Act, 2023, §3(b).

[225] *Id.*, Ch. VIII.

[226] *Id.*, §3(a).

[227] E.U. Regulation 2016/679, *On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free movement of Such Data*, O. J. E. U. L-119/1, Art. 2(1) ('GDPR').

[228] The Digital Personal Data Protection Act, 2023, §3(b)(ii).

[229] *Id*., §2(t); GDPR, *supra* note 227, Art. 9.

[230] The Personal Data Protection Bill, 2019, 373 of 2019, Cl. 2(1)(zc) ('PDP Bill').

[231] The Digital Personal Data Protection Act, 2023, §§27, 33, Sch. I.

[232] Anirudh Burman, *Understanding India's New Data Protection Law*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, October 3, 2023, available at https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (Last visited on December 23, 2024).

[233] PDP Bill, *supra* note 230, Cl. 54; Burman, *supra* note 232.

[234] Burman, *supra* note 232, 8.

[235] Draft Digital Personal Data Protection Rules, 2025, R. 15.

process personal data without consent for executing state functions, including the delivery of government services, fulfilling legal obligations, or ensuring state security. Specifically, §7(b) allows the government to bypass consent requirements if a beneficiary has previously consented to receive another government service. While this simplifies access to personal data for delivering public services, it raises concerns about potential misuse by government agencies by creating aggregated databases.[236] The interplay of these provisions enhances the state's capacity to aggregate, manage, and retain personal data, which scholars caution might result in excessive surveillance and lack of transparency.[237]

Further, the Act grants the central government broad powers to exempt entities from key provisions of the Act, raising concerns about transparency and potential misuse. Under §17(3), the government may exempt certain data fiduciaries, including startups, from compliance with provisions such as lawful data processing (§5), data minimisation (§10), and purpose limitation (§11), without defining the scope, volume, or nature of data processed. Additionally, Section 17(5) allows the government to declare that any provision of the Act will not apply to specified fiduciaries for up to five years from its commencement. However, commentators note that the lack of clear legislative policy or safeguards for these exemptions creates the potential for arbitrary decision-making.[238] Furthermore, concerns have been raised about §36 of the Act, read in conjunction with Rule 22, which grants the government the power to demand information from data fiduciaries or intermediaries without the consent of individuals, for purposes outlined in the Seventh Schedule of the Rules.[239] The criteria for such demands — including the vague and broadly defined interests of national sovereignty, security, and integrity — make it difficult to prevent arbitrary or overreaching use of these powers.

The DPDP Act also grants the government broad discretionary powers in rule-making and oversight, raising concerns about the potential erosion of privacy protections. Unlike the 2019 Data Protection Bill, which proposed an independent Data Protection Authority with rule-making and supervisory functions,[240] the Data Protection Body ('DPB') established under the Act operates under direct government control.[241] The government appoints board members, determines their salaries, and decides their tenure, which is limited to two years with eligibility for reappointment. Such provisions could undermine the DPB's independence and its ability to act against government entities. Furthermore, the Central Government retains exclusive authority to make rules under the Act, as articulated in §40, which enumerates twenty-five specific areas where this power applies. Notably, this list is not exhaustive, leaving the potential for additional areas for delegated legislation. This divergence from international practices like the GDPR, where independent regulatory bodies oversee rule-making and enforcement. Countries like the United Kingdom and Australia also employ overarching legislative frameworks to regulate subordinate rule-making, ensuring transparency and accountability—an approach absent in the Indian context.

Finally, scholars note that the DPDP Act has potentially weakened the Right to Information ('RTI') Act of 2005 — an issue that has also been flagged to the government by

---

[236] *Id*.

[237] Mishra, *supra* note 81, 2; Rubayya Tasneem et al., *Quarterly Transparency Report for October-December 2024: APAAR ID (Again), Digital Media Policy and More*, INTERNET FREEDOM FOUNDATION, December 23, 2024 available at https://internetfreedom.in/quarterly-transparency-report-for-october-december-2024-apaar-id-again-digital-media-policy-and-more/ (Last visited on December 23, 2024).

[238] *Id*.

[239] Draft Digital Personal Data Protection Rules, 2025, R. 22.

[240] PDP Bill, *supra* note 230, Ch. IX.

[241] The Digital Personal Data Protection Act, 2023, §18.

NITI Aayog, the government's top think tank.[242] §44(3) of the DPDP Act amends §8(1)(j) of the RTI Act, which originally allowed public authorities to deny personal information unless public interest justified its disclosure. The amendment removes the public interest exception, restricting the disclosure of personal information under RTI applications, regardless of the public interest. Additionally, the proviso to §8(1)(j) of the RTI Act stated that 'information which cannot be denied to Parliament or a State Legislature shall not be denied to any person'. This ensures that even personal information can be accessed by individuals under RTI if it pertains to parliamentary or legislative matters. The DPDP Act alters this with more restrictive language, further limiting access to such information and curbing the scope of transparency in public authorities.

Notably, the Puttaswamy judgment, which established privacy as a fundamental right, stipulates that any state interference with personal data must meet the strict criteria of legality, necessity, and proportionality.[243] However, the vagueness of terms such as maintenance of public order and security of state under India's data protection framework, combined with the broad discretionary powers granted to the central government and weak oversight and accountability mechanisms threaten to undermine these safeguards. The lack of clarity surrounding these terms, as well as the government's potential for arbitrary decision-making, raises serious concerns about the proportionality and necessity of state intervention in citizens' private affairs.

For India to serve as a credible model for digital governance in the Global South, the DPDP Act must address existing gaps. The broad exemptions granted to government agencies and the expansive powers given to the central government create significant risks of unchecked surveillance, as seen in high-profile incidents like the Pegasus spyware case.[244] While a Supreme Court committee was established to investigate the matter, the government's refusal to fully cooperate emphasises the pressing need for greater accountability and transparency.[245] These issues raise concerns about state-driven digital colonialism, where power dynamics are maintained through surveillance and data control. To create a truly rights-based and inclusive framework, India must implement clearer legislative safeguards aligned with international standards, ensuring privacy protections and limiting governmental overreach. This would not only improve data protection but also contribute to dismantling the historical power imbalances that persist in the digital realm.

B. INTERNET SHUTDOWNS

Another issue confronting the Global South is the frequent recourse to internet shutdowns.[246] India has recorded among the highest number of internet shutdowns globally,

---

[242] Dheeraj Mishra & Soumyarendra Barik, *Govt Ignored Niti Red Flag That Data Protection Law Could Weaken RTI*, THE INDIAN EXPRESS, September 29, 2024, available at https://indianexpress.com/article/india/govt-ignored-niti-red-flag-that-data-protection-law-could-weaken-rti-9593569/ (Last visited on December 23, 2024); Pradip Kashyap, *Digital Personal Data Protection Act, 2023: A New Light Into the Data Protection and Privacy Law in India*, Vol. 2(1), ICREP JOURNAL OF INTERDISCIPLINARY STUDIES, 11 (2023).

[243] Puttaswamy, *supra* note 98.

[244] P.J. George & Saptaparno Ghosh, *Is Pegasus Spyware Targeting Journalists in India*?, THE HINDU, December 29, 2023, available at https://www.thehindu.com/news/national/is-pegasus-spyware-targeting-journalists-in-india/article67683399.ece (Last visited on February 12, 2025).

[245] INDIAN EXPRESS, *SC Pegasus Order: Full Text of the Supreme Court's Judgment*, 2021, available at https://indianexpress.com/article/india/sc-pegasus-order-judgment-full-text-7593039/ (Last visited on 12 February 12, 2025).

[246] ACCESS NOW, *Shrinking Democracy, Growing Violence: Internet Shutdowns in 2023*, May 2024, available at https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf (Last visited on December 23,

frequently citing security and public order concerns.[247] While recent cases in Manipur and Punjab reflect a growing trend, Kashmir has witnessed prolonged blackouts. Similar restrictions in Rajasthan, Haryana, and Uttar Pradesh highlight the urgent need for transparency, oversight, and proportionality in such measures.[248]

Constitutional safeguards serve as guardrails against the misuse of internet shutdowns in India, resulting in litigation before various High Courts and the Supreme Court.[249] In the landmark judgement of *Anuradha Bhasin* v. *Union of India* ('Anuradha Bhasin'), the Supreme Court recognised that Article 19(1)(a) of the Constitution protects the right to disseminate and receive information through the Internet.[250] As a result, any internet shutdown must meet the constitutional standards or reasonable restrictions applied to freedom of speech. These restrictions, outlined in Article 19(2) of the Constitution, require that *firstly,* the restriction be imposed by a valid law; *secondly,* pursue one of the nine grounds specified in Article 19(2); and *thirdly,* be deemed reasonable.

Governments primarily rely on three statutory provisions to impose internet shutdowns: i) §163 of the Bhartiya Nagrik Suraksha Sanhita, 2023, corresponding to §144 of the erstwhile Code of Criminal Procedure, 1973 ('CrPC'); ii) §69A of the IT Act, along with the Information Technology (Procedure and Safeguards for Blocking Access to Information by Public) Rules, 2009 ('Blocking Rules'); and iii) §5(2) of the Telegraph Act, 1885, read with the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 ('Suspension Rules').

A problem with the above legislative framework for internet shutdowns is its fragmented nature.[251] Due to this overlapping framework, authorities invariably proceed under the least procedurally stringent option.[252] What is more, the grounds used for imposing internet shutdowns are overly broad.[253] The resulting interpretive issues regarding the scope of these provisions are exacerbated in the digital sphere. Observers further note that the non-publication

2024); U.N. General Assembly, *Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights: Report of the Office of the United Nations High Commissioner for Human Rights,* U.N. Doc. A/HRC/50/55, (May 13, 2022); Torsha Sarkar et al., *Internet Shutdowns: Threats to Digital Access*, THE CENTRE FOR INTERNET & SOCIETY, October 2020, available at https://www.icnl.org/wp-content/uploads/2.-Internet-Shutdowns-India-report.pdf (Last visited on December 23, 2024).

[247] ACCESS NOW, *India: #KeepItOn – Internet Shutdowns in 2023*, August 26, 2024, available at https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en/ (Last visited on February 12, 2025); Freedom House, *Freedom on the Net 2024: India*, 2024, available at https://freedomhouse.org/country/india/freedom-net/2024 (Last visited on February 12, 2025).

[248] INTERNET SHUTDOWNS, *India's Shutdown Numbers*, available at https://internetshutdowns.in/ (Last visited on February 12, 2025).

[249] *See e.g.*, Anuradha Bhasin, *supra* note 98; Banashree Gogoi v. Union of India, (2019), SCC Online Gau 5584, Foundation of Media Professionals v. Union Territory of Jammu & Kashmir (2020) 5 SCC 746, Faheema Shirin R.K. v. State of Kerala (2019) SCC Online Ker 2976.

[250] Anuradha Bhasin, *supra* note 98, ¶26.

[251] Erica Sharma, *India Requires a Drastic Reform of Its Laws on Internet Shutdowns*, STATECRAFT, April 11, 2021, available at https://www.statecraft.co.in/article/india-requires-a-drastic-reform-of-its-laws-on-internet-shutdowns (Last visited on December 23, 2024).

[252] Nakul Nayak, *The Legal Disconnect: An Analysis of India's Internet Shutdown Laws*, 6 (Internet Freedom Foundation Working Paper No. 1, 2018); Shrutanjaya Bhardwaj, *Rising Internet Shutdowns in India: A Legal Analysis*, Vol. 16(1), I.J.L.T., 122 (2020).

[253] Bhardwaj, *supra* note 252, 136

of shutdown orders is rampant, and even if disclosure is made, it is usually *post facto* through secondary sources like newspapers.[254]

The need for clarity, accountability, and procedural safeguards in implementing internet shutdowns was recognised by the Supreme Court in Anuradha Bhasin. In the context of §69A of the IT Act, the court clarified that the scope of this provision is limited to blocking specific websites and cannot be used to impose blanket internet restrictions.[255] Further, the Court noted that since 2017, states have primarily invoked the Suspension Rules under §5(2) of the Telegraph Act to enforce shutdowns. It ruled that a 'public emergency' is a *sine qua non* for invoking these rules.[256] Additionally, despite the absence of an explicit mandate in the Suspension Rules to publish shutdown orders, the Court required all such orders to be made publicly accessible through an appropriate mechanism to enhance transparency.[257]

Further, the Court reaffirmed the principles of reasonableness, proportionality, and necessity as essential criteria for assessing the legality of internet shutdowns.[258] It emphasised that any restriction must address a 'clear and present danger' and outlined key factors to consider, including the territorial extent of the restriction, the stage and urgency of the emergency, the duration of the measure, and its overall nature.[259] For instance, authorities should prioritise blocking access to specific social media platforms rather than imposing a complete internet shutdown.[260] Moreover, the Court ruled that before invoking the Suspension Rules, the government must assess the stage of the public emergency to ensure that the measure is proportionate, necessary, and the least intrusive option available.[261] The Court also underscored the need for time-bound restrictions under the Suspension Rules. It declared indefinite shutdowns 'impermissible' and recommended that the legislature address the current lack of a maximum time limit for such orders.[262] In the interim, the Court introduced a crucial procedural safeguard: it mandated that the review committee constituted under the Rules conduct a periodic review of suspension orders every seven days.[263] This review must determine whether the shutdown complies with the requirements of §5(2) of the Telegraph Act and assess its proportionality and necessity.[264] These safeguards aim to curb the misuse of internet shutdowns and ensure their alignment with constitutional principles. However, it is worth noting that under the Suspension Rules, the review committee is composed entirely of executive officials (Cabinet Secretary, Secretary of the Ministry of Electronics and Information Technology, and Secretary of the Ministry of Law and Justice at the central level, or their state equivalents).[265] Thus, it remains an executive-dominated body, meaning the government effectively authorises, implements, and reviews its own shutdown orders. Moreover, under the Rules, the committee lacks the authority to set aside suspension orders, raising concerns about the effectiveness of judicial oversight and necessitating appropriate reforms.

---

[254] *Id*.

[255] Anuradha Bhasin, *supra* note 98, ¶111.

[256] *Id*., ¶100.

[257] *Id*., ¶104.

[258] *Id*., ¶¶34–37, 77.

[259] *Id*., ¶¶38,79.

[260] *Id*., ¶111.

[261] *Id*., ¶¶102, 108.

[262] *Id*., ¶¶108–109.

[263] *Id*., ¶109.

[264] *Id*., ¶109.

[265] The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, R. 2(5).

In summary, ensuring transparency, accountability, and adherence to constitutional principles is essential for fostering a rights-based digital ecosystem. The procedural safeguards established by the Supreme Court in Anuradha Bhasin provide a crucial framework for regulating internet shutdowns.[266] These safeguards must be strictly followed to prevent misuse and align such measures with the rule of law.

C. ONLINE CENSORSHIP

Concerns about state-driven digital colonialism in the Global South also arise from online censorship. In line with the Supreme Court ruling in Anuradha Bhasin, online censorship implicates the freedom of speech and expression under Article 19(1)(a) of the Indian Constitution, subject to reasonable restrictions outlined in Article 19(2). In India, the legislative foundation for internet censorship is the IT Act, which criminalises specific online activities, such as publishing obscene material or sharing intimate imagery without consent.[267] The government also has the authority to impose telecommunications and internet shutdowns in certain areas.[268] Previously, §66A of the IT Act penalised sending 'offensive' messages online, but the Supreme Court struck down the provision in *Shreya Singhal* v. *Union of India* ('Shreya Singhal'), citing its vagueness and unconstitutionality.[269]

The principal legal basis for internet censorship in India today is §69A of the IT Act.[270] This provision empowers the central government to block access to specific online content or direct intermediaries to do so. Such action can be taken if it is deemed 'necessary or expedient' to protect national security, the sovereignty and integrity of India, friendly relations with foreign states, public order, or to prevent incitement to cognisable offences related to these grounds. Non-compliance with blocking orders can result in fines and imprisonment of up to seven years.[271] Intermediaries who fail to comply may also risk being held liable as the creators of the prohibited content.[272]

The Blocking Rules prescribe the procedural framework for issuing content-blocking orders. Under the Blocking Rules, a designated official is responsible for receiving blocking requests from various government departments and ministries.[273] These requests are evaluated by a committee comprising secretaries from four ministries and representatives from the Computer Emergency Response Team. The committee assesses whether the request meets the criteria under §69A.[274] Based on the committee's recommendations, the designated official seeks approval from the Ministry of Electronics and Information Technology to issue a blocking order to intermediaries.[275] This procedural framework aims to ensure that content blocking is conducted in accordance with the law and within the scope of §69A.

---

[266] Bhardwaj, *supra* note 252; HUMAN RIGHTS WATCH, *"No Internet Means No Work, No Pay, No Food": Internet Shutdowns Deny Access to Basic Rights in "Digital India"*, June 14, 2023, available at https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic (Last visited on December 23, 2024).

[267] Information Technology Act, 2019, §§67 66E.

[268] The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017.

[269] Shreya Singhal, *supra* note 98.

[270] Information Technology Act, 2000, §69A.

[271] *Id*., §69A(3).

[272] *Id*., §79(3)(b).

[273] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, R. 6 ('Blocking Rules').

[274] *Id.*, R, 7, 8.

[275] *Id.*

Notably, the designated officer is required to make reasonable efforts to identify the 'person or intermediary' hosting the disputed content.[276] If identified, these parties are afforded an opportunity to present their case before the committee within 48 hours.[277] However, this right to a hearing can be bypassed in emergencies where immediate action is necessary.[278] Commentators note that the use of the word "or" in the Blocking Rules implies that either the person or the intermediary may be contacted, but not necessarily both.[279] In practice, this often results in content creators not being informed about the blocking of their material or being given an opportunity to present their case.[280] Transparency issues are further compounded by the confidentiality mandate in the Blocking Rules, which prevents public disclosure of blocking orders.[281] This opacity makes it difficult to assess whether censorship adheres to legal standards, raising concerns about potential misuse of the system.

In Shreya Singhal, the Supreme Court considered the constitutionality of §69A and the Blocking Rules. The petitioners argued that the lack of a mandatory pre-decisional hearing and the confidentiality requirements undermined fundamental rights.[282] They further highlighted the disparity between online censorship and procedural safeguards for censoring physical publications under §§95 and 96 of the CrPC, which mandated the publication of reasoned orders and allowed direct challenges in high courts.[283]

However, the Supreme Court upheld §69A and the Blocking Rules, finding the safeguards they provided to be sufficient.[284] Nevertheless, critics have argued that the Court may have overestimated the consistency with which content creators—when identifiable—are provided with reasoned orders and the opportunity to challenge them in court.[285] This lack of clarity has perpetuated concerns about transparency and procedural fairness in the application of §69A and the Blocking Rules.

In the wake of Shreya Singhal, the government introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('2021 IT Rules'). Critics argue that the 2021 IT Rules reintroduce a framework of broad and vague restrictions on online speech, potentially re-creating the chilling effect that Shreya Singhal sought to eliminate.[286] For instance, the Rules mandate that social media platforms with

---

[276] *Id*., R. 8(1).

[277] *Id*.

[278] *Id*., R. 2(i).

[279] Divyansha Sehgal & Gursdhad Grover, *Online Censorship: Perspectives from Content Creators and Comparative Law on Section 69A of the Information Technology Act*, SSRN (2023), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404965 (Last visited on December 21, 2024).

[280] Apar Gupta, *But What About Section 69A?*, THE INDIAN EXPRESS, March 27, 2015 available at https://indianexpress.com/article/opinion/columns/but-what-about-section-69a/ (Last visited on December 21, 2024); Chinmayi Arun, *The Case of the Online Intermediary*, THE HINDU, September 6, 2016, available at https://www.thehindu.com/opinion/op-ed/shreya-singhal-case-of-the-online-intermediary/article7074431.ece (Last visited on December 21, 2024).

[281] Blocking Rules, *supra* note 273, R. 16.

[282] Shreya Singhal, *supra* note 98, ¶108.

[283] *Id*.

[284] *Id.*, ¶111.

[285] *See* Arun, *supra* note 280.

[286] Tejasi Panjiar & Prateek Waghre, *A Public Brief on the IT Amendment Rules, 2020 a.k.a 'How The Government is Trying to Moderate Online Speech'*, INTERNET FREEDOM FOUNDATION, November 10, 2022, available at https://internetfreedom.in/public-brief-on-the-it-amendment-rules-2022/ (Last visited on February 13, 2025); THE WIRE, *'New IT Rules Against Fundamental Principle of News': Digipub Writes to Prakash Javadekar*, February 26, 2021, available at https://thewire.in/media/digipub-prakash-javadekar-it-rules-digital-

significant user bases to appoint compliance officers and implement traceability mechanisms, raising concerns about their impact on encryption and user privacy.[287] Other examples include Rules 3(1)(b) and 4(4), which require intermediaries to remove content deemed unlawful without judicial oversight, raising concerns about arbitrary takedowns and self-censorship. These Rules also impose stringent due diligence obligations on intermediaries, requiring them to proactively monitor content,[288] appoint grievance officers,[289] and respond to takedown requests within strict timelines.[290] Additionally, digital news publishers and OTT platforms are subject to a three-tier regulatory mechanism, further centralising governmental oversight over online content.[291] While the government maintains that these rules enhance accountability, legal challenges questioning their constitutionality and proportionality continue to unfold in Indian courts.[292] Most of the objections appear to articulate that in seeking to impose these regulations, the 2021 IT Rules are *ultra vires* the parent IT Act as they exceed the scope of what the Act permits, particularly in terms of content blocking and takedown, as well as the regulation of digital media platforms.

The foregoing discussion has highlighted gaps in India's legislative framework concerning privacy and data protection, internet shutdowns, and online censorship. Addressing these issues is crucial for India to realise a rights-based vision of digital sovereignty grounded in the rule of law. By implementing the proposed reforms and procedural safeguards, India can develop a comprehensive digital governance model that effectively counters concerns of state-driven digital colonialism ailing the Global South.

V. CONCLUSION

As a postcolonial digital developmental state, India's approach to digital governance offers a credible model to navigate the complexities underpinning the digital landscape in the Global South. By developing DPI, reclaiming control from dominant platforms, and promoting data governance frameworks aligned with developmental goals, India exemplifies a proactive approach to countering corporate-driven digital colonialism. However, the related challenge of addressing state-driven practices, such as surveillance, censorship, and internet shutdowns, remains significant.

To serve as a credible model for the Global South, India must balance its developmental ambitions with protecting individual rights. In line with this vision, India must strengthen the procedural safeguards as well as ensure transparency and inclusivity in its digital governance processes, with a view to establishing a balanced digital governance framework.

---

media/?ref=static.internetfreedom.in (Last visited on February 13, 2025); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, and Special Rapporteur on the Right to Privacy, 5, U.N. Doc. OL IND 8/2021 (June 11 2021).

[287] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, R. 4(1), R. 4(2).

[288] *Id.*, R. 3(1)(b).

[289] *Id.*, R. 3(2).

[290] *Id.*, R. 3(2)(b).

[291] *Id.*, R. 8–13.

[292] Union of India v. Foundation for Independent Journalism, 2024 SCC Online SC 1196; Kunal Kamra v. Union of India, 2024 SCC Online Bom 3025; Live Law Media Private Limited and others v. Union of India, W.P. (Civil) No. 6272 of 2021 (Kerala High Court) (Unreported).