INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

"RESISTING DIGITAL COLONIALISM THROUGH DATA LOCALIZATION: INDIA'S ASSERTION OF DIGITAL SOVEREIGNTY IN THE INTERNATIONAL LEGAL ORDER"

AUTHORED BY - RASHMI GIRI
Ph.D. Scholar, Faculty of Law, Delhi University

Abstract

The rapid expansion of the digital economy has fundamentally reshaped global power relations, positioning data as a critical resource for economic development, governance, and technological innovation. Yet the benefits of this transformation are unevenly distributed. The contemporary global digital order is marked by deep structural asymmetries in data ownership, infrastructure, and value extraction, disproportionately favouring transnational technology corporations and states located in the Global North. These dynamics have given rise to what scholars increasingly describe as digital colonialism—a system of domination in which data generated in the Global South is extracted, processed, and monetized under foreign control, often beyond the reach of domestic regulation.

This article examines data localization as a legal and constitutional response to digital colonialism, with a particular focus on India's evolving data governance framework. It argues that data localization should not be understood merely as a protectionist or efficiency-reducing measure, but as a strategic assertion of digital sovereignty aimed at reclaiming regulatory authority, safeguarding fundamental rights, and addressing historical patterns of digital dependency. Drawing on international law, constitutional theory, and political economy, the paper situates data localization within broader debates on sovereignty in the digital age, where territorial jurisdiction is increasingly challenged by borderless data flows.

Using India as a case study, the article analyses the constitutional foundations of digital sovereignty, particularly the role of Articles 19 and 21 of the Indian Constitution and the Supreme Court's recognition of the right to privacy in Justice K.S. Puttaswamy v. Union of India. It examines India's hybrid data localization model, encompassing sector-specific mandates and the Digital Personal Data Protection Act, 2023, and evaluates its implications for global data governance.

ISSN: 2582-6433

The article concludes that while data localization is not a comprehensive solution to digital colonialism and carries risks of regulatory overreach, it constitutes a legitimate and constitutionally grounded tool through which developing states can contest asymmetrical digital power structures and contribute to the reconfiguration of a digital legal order.

Keywords: Digital Colonialism, Data Sovereignty, Data Localization, Data Protection, Data Governance.

I. Introduction

The digital transformation of economies and societies has profoundly altered the distribution of power in the international legal order. Data once an ancillary by-product of human activity has emerged as a strategic resource central to economic growth, political authority, and social governance. States, corporations, and international institutions increasingly recognize that control over data determines competitiveness in artificial intelligence, financial markets, public administration, and national security.

Yet this transformation has not occurred on equal terms. The global digital economy is marked by stark asymmetries in ownership, control, and value extraction, disproportionately favouring a small number of transnational technology corporations and states located primarily in the **Global North**[1]. Vast quantities of data generated by individuals, businesses, and public institutions in the **Global South** are routinely extracted, processed, and monetized abroad, often beyond the effective reach of domestic regulation.

This imbalance has given rise to the concept of "**digital colonialism,** a term used to describe contemporary forms of domination enabled through data extraction, digital infrastructure control, and platform governance". Unlike traditional colonialism, which relied on territorial conquest and formal political subjugation, digital colonialism operates through private power, contractual arrangements, technological dependency, and international legal norms that privilege unrestricted cross-border data flows.[2]

[1] Zymone Ellery A. Reyes, *Digital Colonialism: Big Tech's Grip on Sovereignty in a Globalized Era*, De La Salle University (2024) https://www.researchgate.net/publication/387160844_Digital_Colonialism_Big_Tech's_Grip_on_Sovereignty_in_a_Globalized_Era.

[2] Nothias Toussaint, *An intellectual history of digital colonialism*, 27 J. COMM. 385, 388 (2025).

ISSN: 2582-6433

Data generated by individuals and institutions in the Global South is routinely harvested, processed, and monetized by foreign entities. These mechanisms undermine the regulatory autonomy of developing states and erode their capacity to "protect privacy, ensure national security, and preserve economic value" from data generated within their territories.

The rise of digital colonialism poses profound challenges to the classical conception of **sovereignty**. Sovereignty in international law has historically been anchored in territorial jurisdiction and the principle of non-intervention. However, in a digital environment where data flows seamlessly across borders and critical infrastructure is privately owned, states particularly developing states struggle to exercise effective control over activities affecting their citizens and economies. As a result, sovereignty is increasingly fragmented, diluted, and reconfigured.

In response, **data localization** has emerged as a prominent regulatory strategy. By requiring that certain categories of data be stored or processed within national borders, states seek to reclaim regulatory authority, protect privacy, ensure national security, and promote domestic digital industries[3]. While often criticized as protectionist or inefficient, data localization reflects deeper concerns about autonomy, dignity, and structural inequality in the global digital order.

This article examines whether "data localization can function as a legal tool to resist digital colonialism and reassert sovereignty" within the international legal order, using India as a case study. It argues that India's data localization measures represent a constitutionally grounded assertion of digital sovereignty that challenges prevailing international legal norms favouring unrestricted cross-border data flows. While data localization is "neither a panacea nor free from risks", India's approach illustrates how developing states can deploy law to contest asymmetrical digital power structures and reimagine sovereignty in the digital age.

II. Conceptual Foundations of Digital Colonialism and Reimagining Sovereignty in the Digital Age

1. From Traditional Colonialism to Digital Colonialism

The 21st century has witnessed the emergence of 'digital colonialism'—a concept describing how contemporary digital infrastructures and data practices replicate and extend patterns of

[3] Anirudh Burman, and Upasana Sharma, *History of Data Localization. How Would Data Localization Benefit India?* Carnegie Endowment for International Peace (2021) http://www.jstor.org/stable/resrep31117.4.

ISSN: 2582-6433

historical colonialism through the extraction, control, and monetisation of data by powerful actors predominantly based in the Global North[4]. Digital colonialism can be best understood as an evolution rather than a rupture from historical colonial practices[5].

Classical colonialism involved the extraction of natural resources, labour, and wealth from colonized territories, justified through legal doctrines such as terra nullius and civilizational hierarchies. Colonized societies were incorporated into global economic systems designed to benefit imperial centers, leaving enduring legacies of underdevelopment and dependency.[6]

In the digital age, data has replaced land and minerals as the primary extractive resource. Individuals and institutions in the Global South generate vast quantities of data through everyday activities—communication, consumption, financial transactions, and governance[7]. This data is captured by digital platforms, transferred across borders, and processed using advanced computational infrastructure located predominantly in the Global North. This dynamic reshapes global power relations, undermines state sovereignty in the Global South, and reveals significant gaps in international law's ability to confront structural inequalities in the digital age.[8] The resulting economic value, innovation, and strategic advantage accrue largely to foreign corporations and states.

The continuity between traditional and digital colonialism lies in **structural asymmetry**. In both cases, the periphery supplies raw material while the core controls processing, governance, and profit.[9] The difference lies in form rather than substance: digital colonialism is less visible, more normalized, and embedded in seemingly neutral technical and legal frameworks. Yet the underlying logic remains extractive and unequal: the wealth and control generated from colonised territories are redirected to dominant powers.[10]

In the digital era, data functions as a new primary resource, replacing land and minerals as the foundation of value creation. Corporations such as Google, Meta, Amazon, and Microsoft own the platforms, cloud infrastructure, and algorithms through which raw data from billions of users in developing countries are siphoned, analysed, and monetised.[11] This mirrors colonial trade systems, where colonies supplied raw materials that were processed and sold by imperial

[4] Zymone Ellery A. Reyes, *Supra* note 1.
[5] Özgür Yılmaz, *The Origins of Digital Colonialism*, 16 İMGELEM J. 321, 323 (2025).
[6] *Id.*
[7] Nothias Toussaint, *supra* note 2 at 389.
[8] Anirudh Burman, *supra* note *3*.
[9] Bitange Ndemo, *Addressing digital colonialism: A path to equitable data governance*, UNESCO Inclusive Policy Lab (Aug. 8, 2024) https://en.unesco.org/inclusivepolicylab/analytics/addressing-digital-colonialism-path-equitable-data-governance
[10] *Id.*
[11] Özgür Yılmaz, *supra* note 5 at 327.

ISSN: 2582-6433

powers, leaving local economies dependent and marginalised.

2. Data Sovereignty in the Digital Age

Classical sovereignty in international law encompasses territorial integrity, political independence, and the right to regulate within borders. Sovereignty has long been the organizing principle of international law. Rooted in the Peace of Westphalia, it presupposes that states possess supreme authority within defined territories and enjoy formal equality in the international system[12]. However, the digitization of social and economic life destabilizes this model.

As data generated within a state's territory is stored and processed on foreign servers, often under foreign jurisdiction, states lose regulatory control over information critical to economic and political governance.[13] Data flows challenge territoriality. A single digital transaction may involve multiple jurisdictions, private intermediaries, and automated decision-making systems. When data is stored abroad, domestic regulators face significant obstacles in enforcing privacy laws, taxation, competition policy, and criminal investigations.[14] This erosion of effective control undermines the substantive content of sovereignty, particularly for states with limited bargaining power.

In response, **data sovereignty** has emerged as both a legal and political concept. It refers to a state's capacity to regulate data generated within its jurisdiction, including its collection, storage, processing, and transfer.[15] For developing states, data sovereignty is closely linked to development, as data-driven technologies increasingly determine economic trajectories and governance capacity. Many nations are adopting data localisation and privacy laws as expressions of this principle to ensure that data remains subject to domestic legal frameworks and to protect individual rights.

Yet, such measures are often defensive responses to power asymmetries rather than comprehensive solutions. Data localisation can slow cross-border flows but does not automatically empower local economies to process, interpret, or derive value from data at scale, especially when computational infrastructure and AI capabilities remain concentrated in the Global North.[16]

---

[12] Hongfei Gu, *Data, Big Tech, and the New Concept of Sovereignty*, 23 J. CHINESE POL. SCI. 591, 592 (2023).
[13] Mansi Rathi, *Digital Colonialism: Examining the Extraterritorial Impact of Tech Giants and State Sovereignty*, LEGAL QUORUM (Aug. 23, 2025) https://thelegalquorum.com/digital-colonialism-examining-the-extraterritorial-impact-of-tech-giants-and-state-sovereignty/
[14] *Id.*
[15] Hongfei Gu, *supra* note 12, at 595.
[16] Nothias Toussaint, *supra* note 2, at 390.

ISSN: 2582-6433

3. Global Data Flows and North–South Asymmetries

The dominant narrative surrounding global data flows emphasizes efficiency, innovation, and global connectivity. However, this narrative obscures how data flows reinforce existing inequalities. According to recent analysis, the majority of the world's data centres—and thus the infrastructure for storage and processing—are located in the United States and Europe, while developing regions host a fraction of these facilities[17]. This means that even when data originates in the Global South, its control, analysis, and economic value accrue disproportionately to entities outside those jurisdictions. Developing states often lack the infrastructure, capital, and legal leverage to retain data or capture its value. Meanwhile, Global North corporations benefit from economies of scale, proprietary algorithms, and favorable trade rules.

This asymmetry is compounded by platform capitalism—where companies extract not only data but also behavioural insights and predictive power to refine products, target users, and shape economic outcomes.[18] These capabilities are deeply embedded in AI development, enabling Global North firms to maintain competitive advantages in emergent technologies **United Nations Conference on Trade and Development (UNCTAD)** reports consistently highlight that the digital economy is characterized by winner-takes-all dynamics, with data concentration exacerbating global inequality.[19] In this context, unrestricted data flows function less as neutral conduits of innovation and more as mechanisms of resource extraction.

In the absence of equitable governance, the digital economy reproduces patterns of dependency: the Global South contributes raw digital labour and data, but value creation, algorithmic innovation, and monetisation occur elsewhere. This is reflected in case studies across Africa, Latin America, and Asia, demonstrating how local digital initiatives remain tethered to foreign platforms and technologies, constraining autonomous development.[20]

4. Big Tech Dominance and the Absence of Regulation

Big Tech corporations increasingly exercise quasi-sovereign power. They regulate speech, shape markets, and influence democratic processes through platform design and algorithmic governance. Yet international law provides few tools to hold them accountable. Their

[17] Michael Kwet, *Digital colonialism: US empire and the New Imperialism in the Global South*, 60 RACE & CLASS 3, 4-13 (2019).
[18] *Id* at 16.
[19] United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report*, UNCTAD/DER/2021 (Sep. 29, 2021) https://unctad.org/system/files/official-document/der2021_en.pdf
[20] Michael Kwet, *supra* note 17, at 19.

ISSN: 2582-6433

dominance affects national policy spaces, limiting the ability of developing states to regulate privacy, competition, and digital rights without facing resistance from powerful corporate interests.[21] There is no binding multilateral framework governing cross-border data governance, platform responsibility, or digital monopolies.

This regulatory vacuum disproportionately harms developing states. Without explicit recognition of digital colonialism or data extractivism, international law tacitly legitimizes existing power asymmetries, undermining the principle of sovereign equality.[22]

This influence challenges the essence of sovereignty, not only by decentralising regulatory authority but also by embedding foreign priorities into domestic decision-making processes. As digital ecosystems become integral to governance—through e-government systems, identity platforms, and critical infrastructure—states without robust countervailing capacities risk being subject to external governance rationalities.[23]

III. Constitutional Foundations of Digital Sovereignty in India

India's assertion of digital sovereignty is not merely a policy choice but is deeply embedded in its constitutional framework and judicial philosophy. The Indian Constitution, through its guarantees of fundamental rights and its federal structure, provides a normative framework for asserting control over data flows and digital infrastructure.[24]

1. Article 19 and the Digital Public Sphere

Although the Constitution of India does not explicitly refer to data or "digital sovereignty," several constitutional provisions are directly implicated. Article 19, which guarantees freedoms such as speech, expression, and trade, plays a dual role in the digital context[25]. On the one hand, digital platforms expand expressive freedoms; on the other, unregulated digital ecosystems dominated by foreign actors may distort public discourse and undermine democratic participation.

Reasonable restrictions under Article 19(2) thus provide constitutional space for regulating digital platforms in the interests of sovereignty, public order, and security.[26] Data localization can enhance regulatory oversight over platforms operating within India, enabling the protection

[21] Zymone Ellery A. Reyes *supra* note 1.
[22] Bitange Ndemo, *supra* note 9.
[23] Özgür Yılmaz, *supra* note 5 at 327.
[24] Ch. Venkateswarlu, *The Constitutional Safeguards for the Right to Privacy in the Digital Era*, 5 IND. J. INTE. RES. LAW. 1359, 1362-68 (2025).
[25] India Const. art. 19.
[26] India Const. art. 19, cl. 2.

ISSN: 2582-6433

of constitutional freedoms.

2. Article 21 and the Right to Privacy

Article 21, which guarantees the right to life and personal liberty, has been expansively interpreted to include dignity, autonomy, and privacy[27]. In the digital age, personal data has become integral to individual autonomy. The extraction, processing, and monetization of data without adequate safeguards threaten informational self-determination, making data governance a constitutional concern rather than a purely economic one.[28]

In **Justice K.S. Puttaswamy v. Union of India (2017)[29]**, the Supreme Court of India unequivocally recognized the right to privacy as a fundamental right under Article 21. The Court emphasized that privacy is intrinsic to dignity, autonomy, and self-determination. Importantly, it acknowledged the dangers posed by unregulated data collection and processing by both state and private actors.[30]

Before **Puttaswamy,** privacy was neither expressly guaranteed in the Constitution nor uniformly recognized by courts. Early cases like **Kharak Singh v. State of Uttar Pradesh (1962)** dismissed privacy claims under Articles 19 and 21, reflecting a narrow understanding of personal liberty.[31]

The Court emphasized that privacy includes *informational privacy* —the ability of individuals to control how their personal data is collected, stored, and used. This doctrinal shift was indispensable in confronting digital phenomena such as mass surveillance, biometric databases, and unauthorized data aggregation, all of which pose existential threats to privacy if left unchecked.[32]

Moreover, the Court articulated a *proportionality test* for privacy intrusions—requiring legality, a legitimate state objective, and proportional means—thereby mandating that any state or non-state interference with data or personal information must meet strict constitutional scrutiny.[33] This framework informs India's data protection regime and supports state measures aimed at preventing unchecked cross-border data exploitation that could undermine constitutional rights.

---

[27] India Const. art. 21.
[28] Ch. Venkateswarlu, *supra* note 24.
[29] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[30] *Id.*
[31] Kharak Singh v. State of Uttar Pradesh, (1963) AIR 1295.
[32] Ayush Chandra, *Right to Privacy and Article19 and 21 of the Constitution*, LEGALONUS (Aug. 31, 2023) https://legalonus.com/right-to-privacy-and-article19-and-21-of-the-constitution/.
[33] *Id.*

ISSN: 2582-6433

3. Federalism and India's Data Governance Approach

India's federal structure adds another dimension to data sovereignty. While the Union exercises powers over communications[34] and national security[35], states increasingly rely on data-driven systems for welfare delivery, policing, and public services. This creates a constitutional imperative to balance centralized digital control with federal autonomy, reinforcing the need for sovereign oversight over digital infrastructure and data flows.

India's approach to data governance is increasingly shaped by constitutional commitments to dignity, accountability, transparency, and welfare-oriented governance. Rather than viewing data merely as an economic asset, recent policy frameworks conceptualize data as a public resource capable of enhancing democratic governance and service delivery, provided it is regulated in a rights-respecting manner.[36]

The **Draft National Data Governance Framework Policy** articulates a vision of data-led governance, aimed at improving efficiency and inclusiveness in public administration across sectors such as health, agriculture, education, and justice.[37] This approach aligns with constitutional values implicit in Articles 14 and 21, which demand non-arbitrariness, transparency, and protection of personal liberty. By emphasizing standardized data management practices, interoperability, and accountability of public institutions, the framework seeks to embed good governance principles into the digital state.[38]

Constitutional values also require that data governance protect individual autonomy and informational self-determination. As large-scale data processing becomes integral to welfare delivery and policymaking, safeguards relating to consent, purpose limitation, and data security acquire constitutional significance.[39] The evolving statutory framework, including the Digital Personal Data Protection Act of 2023, reflects this shift by imposing obligations on data fiduciaries and recognizing the rights of individuals over their personal data.

At the institutional level, the creation of centralized data governance bodies and uniform standards is intended to enhance transparency and public trust while ensuring sovereign

[34] India Const. List I- Union List, Item 31.
[35] India Const. List I- Union List, Item 9.
[36] Mayank Chaurasia, *Data Governance and Organizational responsibility under India's new digital laws*, 3 IND. J. RES. LAW & MAN. (Jan. 27, 2026) https://ijrlm.com/journal/data-governance-and-organizational-responsibility-under-indias-new-digital-laws/.
[37] MINISTRY OF ELEC. AND INFO. TECH., GOV'T OF INDIA, DRAFT NATIONAL DATA GOVERNANCE FRAMEWORK POLICY (Issued on July 27, 2022). https://www.meity.gov.in/content/draft-national-data-governance-framework-policy.
[38] Prashant Kumar Mittal, Mukesh Kumar Gupta & Shashi Kant Pandey, *Decoding Data Governance & Strategy*, INFORMATICS (Apr. 2025) https://informatics.nic.in/files/websites/april-2025/decoding-data-governance-strategy.php. [hereinafter *Decoding*]
[39] Ch. Venkateswarlu, *supra* note 24, *at 1369.*

ISSN: 2582-6433

oversight over data ecosystems[40]. However, constitutional concerns persist regarding democratic participation and oversight. Data governance regimes that prioritize state utility or innovation without adequate citizen involvement risk diluting constitutional guarantees of accountability and dignity.[41]

IV. Data Localization as Resistance to Digital Colonialism

1. Defining and Classifying Data Localization

Data localization has become a central feature of contemporary digital regulation, often portrayed as a form of digital protectionism. However, when examined through the lens of digital colonialism, localization emerges as a strategic response to structural asymmetries embedded in global data flows.[42]

In the context of digital colonialism where data generated in the Global South is extracted, processed, and monetized by actors in the Global North data localization emerges not merely as a regulatory technique, but as a form of legal resistance through which states in the Global South seek to reclaim sovereignty, autonomy, and regulatory authority over data as a critical resource in the international digital economy.[43]

At its core, data localization refers to legal or regulatory requirements mandating that data be stored, processed, or retained within a country's territorial boundaries[44]. Localization regimes vary in scope and intensity. Data localization encompasses a spectrum of regulatory approaches:

a) **"Strict localization** requires all data to be stored and processed domestically, with minimal or no cross-border transfer".

b) **"Partial localization** permits cross-border data flows subject to conditions such as regulatory approval or mirroring requirements."

c) **"Sectoral localization** applies only to specific categories of data—such as financial, health, telecommunications, or critical infrastructure data—reflecting differentiated regulatory priorities".

Comparative studies show that most states adopt hybrid or sector-specific approaches rather

[40] *Id.*
[41] *See, Decoding, supra* note 38.
[42] *Data Sovereignty, Data Residency, and Data Localization: An Introduction,* https://www.scalecomputing.com/documents/Data-Sheets/SC_Data-Sovereignty_7-23.pdf (last visited Feb. 28, 2026). [hereinafter *Data Sovereignty*]
[43] KAUSHAMBI BAGCHI, GANGESH VARMA & SASHANK KAPILAVAI, INDIAN COUNCIL FOR RES. ON INT'L ECO. RELATIONS, DATA FLOWS AND DATA LOCALISATION: AN ECONOMIC ANALYSIS 2-6 (2020).
[44] *See, Data Sovereignty, supra* note 42.

ISSN: 2582-6433

than absolute bans, reflecting a balance between sovereignty and economic integration[45]. Critics say hard localization would mean inefficiencies, overlaps, and delays of services. India has largely adopted partial and sectoral localization i.e., a hybrid model of localization, reflecting a calibrated approach.

2. Data Localization as a Constitutional Imperative

Under data localization the requirement that certain categories of data be stored or processed within national territory is often criticized as restrictive or incompatible with global data flows.[46] However, within India's constitutional framework, data localization can be understood as a mechanism for preserving constitutional autonomy, dignity, and democratic self-governance[47]. When designed proportionately and transparently, localization measures serve legitimate constitutional objectives rather than arbitrary state control.

By ensuring that sensitive personal and public data remain subject to Indian jurisdiction, data localization enhances the enforceability of constitutional rights, judicial oversight, and democratic accountability[48]. It reduces dependence on foreign legal systems and corporate governance structures that may not align with India's constitutional values. In this sense, data localization is not merely a regulatory tool but a constitutional strategy to safeguard informational self-determination.[49]

3. Normative and Theoretical Justifications

The theoretical justifications for data localization are rooted in multiple dimensions of state authority. From a sovereignty perspective, control over data is increasingly analogous to control over strategic resources. National security concerns arise where sensitive data stored abroad becomes subject to foreign surveillance or extraterritorial legal regimes. Privacy and informational self-determination further justify localization by enhancing enforceability of domestic data protection laws.[50] Finally, economic self-determination supports localization as a means to retain value derived from data, foster domestic digital industries, and reduce dependency on foreign platforms.[51]

---

[45] Rana Saurav Kumar Singh, et.al., *Data Localization And Its Impact On Cross-Border Digital Trade In India: Legal, Economic, And Strategic Implications*, 30 EDUCATIONAL ADMINISTRATION: THEORY AND PRACTICE 3326, 3328 (2024). [hereinafter *Data Localization*]
[46] *Id.*
[47] Mansi Rathi, *supra* note 13.
[48] *See, Data Sovereignty, supra* note 42.
[49] *See, Data Localization, supra* note 45 at 3329.
[50] KAUSHAMBI BAGCHI, ET.AL., *supra* note 43, at 22.
[51] Anirudh Burman, *supra* note 3.

ISSN: 2582-6433

Despite these justifications, data localization faces substantial criticism. Critics argue that localization fragments the internet, undermines its open and global character, and creates trade barriers that hinder innovation and efficiency.[52] Increased compliance costs, reduced economies of scale, and potential retaliation through trade regimes are frequently cited concerns[53].

However, these critiques often assume a neutral global digital marketplace, obscuring the structural dominance of Global North actors that benefit from unrestricted data flows. From a Global South perspective, these justifications are intertwined with historical experiences of exploitation and dependency.

4. Localization as Counter-Hegemonic Strategy

Reframed through a postcolonial lens, data localization can be positioned not as protectionism but as a counter-hegemonic legal strategy. In a global order where data extractivism mirrors historical resource extraction, localization represents an attempt to rebalance power and assert regulatory agency.[54] It challenges the presumption that free data flows are universally beneficial and questions whose interests such openness truly serves. By asserting control over data, states contest the privatization of sovereignty.

Data localization also functions as a tool to counter foreign surveillance and data extractivism. When data is stored under foreign jurisdictions, it may be accessed by external governments or corporations without meaningful accountability[55]. Keeping data within national borders enhances judicial oversight and democratic accountability.

Moreover, localization strengthens domestic regulatory capacity by enabling regulators to audit, enforce, and supervise data practices more effectively.[56] *"For instance, regional regulatory models such as the European Union's General Data Protection Regulation (GDPR) impose strict conditions on the transfer of personal data to foreign jurisdictions lacking adequate privacy safeguards".* It facilitates compliance monitoring, consumer protection, and competition regulation, particularly in markets dominated by transnational platforms.

---

[52] Oskar Szydłowski, *Digital Protectionism: Data Localisation* (Dec. 22, 2021) https://pism.pl/publications/digital-protectionism-data-localisation.

[53] *Id.*

[54] Erol Yayboke, Carolina G. Ramos & Lindsey R. Sheppard, *The Real National Security Concerns over Data Localization*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (July 23, 2021) https://www.csis.org/analysis/real-national-security-concerns-over-data-localization.

[55] *Data Localization and Global Privacy Laws: How to Manage the Regulatory Patchwork*, https://trustarc.com/resource/data-localization-global-privacy-laws/. (last visited Feb. 29, 2026). [hereinafter *Privacy Laws*]

[56] *Id.*

ISSN: 2582-6433

Finally, some policymakers view localization as part of broader digital industrial policy aimed at nurturing domestic data economies, creating jobs in data infrastructure, and supporting local technology ecosystems.[57] While such objectives can yield domestic economic benefits, they also risk erecting barriers to international trade in digital services.

Nonetheless, data localization is not without risks. Poorly designed regimes may enable state overreach, mass surveillance, or censorship. Additionally, infrastructural dependence—where domestic capacity remains reliant on foreign technology—can undermine the objectives of localization.[58] Without parallel investment in infrastructure and safeguards, localization alone cannot dismantle digital dependency. Thus, localization must be embedded within a rights-based constitutional framework.

V. India's Data Localization Framework and the Reconfiguration of Global Data Governance

The governance of cross-border data flows has emerged as one of the most contested issues in contemporary international law and global political economy. Long dominated by the doctrine of the free flow of data, global data governance is increasingly marked by assertions of sovereign control, regulatory pluralism, and fragmentation.[59] India's evolving data localization framework represents a significant intervention in this shifting landscape. By prioritizing regulatory autonomy, privacy, and national interests, India challenges prevailing liberal assumptions and contributes to the reconfiguration of global data governance.[60]

1. Legal Foundations of Data Localization in India

India's data localization regime is anchored primarily in two legal instruments: the **Digital Personal Data Protection Act, 2023 (DPDP Act)** and sector-specific mandates issued by regulatory authorities, like the **Reserve Bank of India (RBI)** and **Insurance Regulatory and Development Authority of India (IRDAI).** The DPDP Act establishes a comprehensive framework for the protection of personal data, permitting cross-border data transfers subject to conditions prescribed by the central government.[61] While the Act does not impose blanket localization requirements, it retains sovereign discretion over data transfers, reflecting concerns

[57] Joesph Werner, *Cross-Border Data Flows and Data Localization Policies: Economic, Legal, and Regulatory Perspectives*, RESEARCH GATE (Jan. 2, 2026) https://www.researchgate.net/publication/399359338_Cross-Border_Data_Flows_and_Data_Localization_Policies_Economic_Legal_and_Regulatory_Perspectives.
[58] Erol Yayboke, *supra* note 54.
[59] Joesph Werner, *supra* note 57.
[60] *See, Data Localization*, *supra* note 45 at 3330.
[61] The Digital Personal Data Protection Act, 2023, §16.

ISSN: 2582-6433

related to privacy, security, and regulatory oversight.[62]

Operationalizing the DPDP Act depends on the **Digital Personal Data Protection Rules, 2025,** which the government has notified to clarify implementation details. These Rules empower the government to identify classes of data that must remain within India for specified purposes and apply localization requirements to significant data fiduciaries, entities processing large volumes of Indian personal data thereby embedding localization into the operational fabric of India's data protection regime.[63]

The IT Act does not mandate data localisation; it provides for certain practices that corporations and individuals who collect, receive, possess, store, deal with, or handle information of persons must adopt through the rules prescribed therein. Section 67C of the IT Act requires intermediaries to keep certain data for specific time periods and formats as determined by the government.[64] The IT SPDI Rules provide for transferring sensitive personal data or information outside India as long as those countries ensure the same level of data protection and uphold confidentiality agreements[65]. The latest in line is the IT Intermediary Guidelines 2021, require intermediaries to hand over user-related data to relevant authorities upon official request, which poses challenges when data is stored out of the country.[66]

In contrast, the RBI's data localization mandates particularly in relation to payment system data require that certain categories of financial data be stored exclusively within India.[67] Similarly, the IRDAI (Maintenance of Insurance Records) Regulation, 2015, requires covered organizations to store insurance data within India[68]. These mandates are justified on grounds of consumer protection, financial stability, and effective regulatory supervision.

Draft policies and existing guidelines in sectors like e-commerce and telecommunications have also hinted at data localisation norms. The Digital Health Data Management Policy, *for instance*, recommends storing critical health data within India[69]. Companies operating in these sensitive sectors must be prepared for a tightening of norms.

However, this approach raises questions of coherence and consistency. The coexistence of permissive transfer regimes under the DPDP Act and strict localization requirements in specific

[62] *Id.* §17.
[63] The Digital Personal Data Protection Rules, 2025, r.22.
[64] Information Technology Act, 2000, § 67C.
[65] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
[66] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[67] RBI's Directive 2017-18/153 (April 6, 2018) issued under the Payment and Settlement Systems Act 2007, §2(i).
[68] IRDAI (Maintenance of Insurance Records) Regulation, 2015, para. 3(9).
[69] Pritam Sen, *Data Localization: An Issue in the Cross-Border Digital Economy*, 5 INDIAN J. INT. RES. LAW. 1512, 1518 (2025).

ISSN: 2582-6433

sectors creates regulatory complexity. While flexibility allows regulators to tailor rules to sectoral risks, it also generates uncertainty for firms and complicates compliance. India's localization framework thus reflects an incremental and fragmented regulatory strategy rather than a singular localization doctrine.[70]

2. Global Data Localization Trends and Comparative Models

Globally, data localization has moved from being an exception to becoming a mainstream regulatory tool. Across jurisdictions, governments have sought to assert greater control over data generated within their territories, motivated by concerns relating to privacy protection, national security, economic sovereignty, and regulatory enforcement[71]. As a result, global data governance is no longer shaped by a singular commitment to unrestricted cross-border data flows but by a plurality of regulatory models reflecting diverse political, economic, and constitutional priorities. A comparative examination of India, Brazil, China, and the European Union localization models highlights the divergent approaches.

Brazil, through its General Data Protection Law ((Lei Geral de Proteção de Dados – known as the LGPD), adopts a comparatively liberal approach. Rather than mandating localization, Brazil emphasizes lawful data transfers based on consent, adequacy, and contractual safeguards. Its model prioritizes data protection and interoperability over territorial data control, positioning Brazil closer to global data flow norms while retaining regulatory oversight.[72]

China represents the most stringent model, embedding data localization within a broader framework of cybersecurity and national security law. Article 37 of the Cybersecurity Law (2017), that Critical Information Infrastructure (CII) operators keep domestic servers that store all personal data and so-called important data collected in China.[73] The requirements cover areas like public communication, finance, energy, and government, with cross-border transfers permitted only following a rigorous security assessment.[74] Its regime mandates extensive domestic storage of data and grants the state wide powers of access and control. This security-centric approach prioritizes state authority over market openness.

The European Union, by contrast, adopts a conditional transfer model under the General Data

[70] *Id.* at 1515.
[71] Oskar Szydłowski, *supra* note 52.
[72] *Brazil's Data localization and regulation of non-personal data,* https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/latin-america/brazil/topics/data-localization-and-regulation-of-non-personal-data (last visited Feb. 29, 2026).
[73] Cybersecurity Law of the People's Republic of China, art. 37 (2017).
[74] *Id.*

ISSN: 2582-6433

Protection Regulation (GDPR)[75]. While not mandating strict localization, the EU restricts data transfers to jurisdictions that meet its adequacy standards or provide appropriate safeguards. Data transfers to countries outside the European Economic Area (EEA) are only permitted when those countries have appropriate levels of protection or in place adequate safeguards such as "Standard Contractual Clauses" (SCCs) and Binding Corporate Rules.[76] To circumvent these difficulties, most companies store data inside the EEA, thereby achieving de facto localization.

India's model occupies a middle position. It neither fully embraces China's security-driven localization nor Brazil's or EU's harmonized transfer regime. Instead, it is characterized by a hybrid model combining economy-wide data protection legislation with sector-specific mandates.[77] It relies on selective localization combined with sovereign discretion over data flows, reflecting a balance between openness and control.

Together, these comparative models illustrate the growing fragmentation of global data governance and the emergence of multiple regulatory pathways beyond the free flow of data paradigm[78].

3. Challenging the Free Flow of Data Doctrine

India's embrace of data localization represents a critical challenge to the long-established doctrine of "the free flow of data" a principle that has underpinned global digital trade, innovation, and economic integration[79]. Traditionally, international governance, including trade agreements and multilateral frameworks, has promoted the unfettered movement of data across borders to maximize economic productivity, foster innovation, and enable seamless global services.[80]

However, as states increasingly assert digital sovereignty, this doctrine is being contested both in rhetoric and regulatory practice. India's data localization framework exemplifies this shift, exposing fundamental tensions between regulatory objectives and the practical challenges of implementation.

Data localization policies often arise from competing regulatory objectives that expose inherent tensions between openness and control. On one hand, the state seeks to enhance privacy protection, ensure law-enforcement access to data, and mitigate national security risks

[75] General Data Protection Regulation (GDPR), 2018. (European Union)
[76] Erol Yayboke, *supra* note 54.
[77] Pritam Sen, *supra* note 69, at 1519.
[78] *See, Privacy Laws, supra* note 55.
[79] *See, Data Localization, supra* note 45 at 3330.
[80] Joesph Werner, *supra* note 57.

ISSN: 2582-6433

associated with foreign data storage and surveillance[81]. On the other hand, localization introduces compliance burdens, infrastructural demands, and potential inefficiencies that complicate participation in the global digital economy.[82] This dynamic complicates the regulatory landscape, as policymakers struggle to balance the economic benefits of cross-border data mobility with sovereign claims to protect domestic interests. Yet, these objectives often collide with the operational realities of globally integrated digital services, creating regulatory friction and uncertainty.

The European Union's approach rooted in the GDPR's adequacy and safeguards framework does not outright reject cross-border data flows but conditions them on equivalence of privacy protections.[83] This reflects a more rights-based model that still supports data mobility, albeit within stringent regulatory parameters. In contrast, China's model imposes "hard localization and security reviews", asserting comprehensive territorial control over data as part of broader national sovereignty objectives.

Comparatively, by asserting regulatory control over data, India positions itself as a norm challenger in global data governance. India's hybrid approach selectively challenges liberal data flow norms without fully retreating into digital isolationism. By imposing localization requirements whether through sector-specific mandates or conditional restrictions on data transfers the state signals a departure from the free flow paradigm.[84] These measures reflect India's efforts to assert regulatory oversight, strengthen law enforcement access to data, and protect citizens' digital rights within its jurisdiction.

However, the practical effect is to reconfigure the normative underpinnings of global data governance, privileging sovereign control over seamless cross-border data exchange. In doing so, India approach must be understood within broader Global South efforts to reshape international digital norms. Across **Asia, Africa, and Latin America**, states are increasingly contesting governance models historically shaped by Global North interests and platform dominance.[85] For many developing countries, unrestricted data flows have facilitated large-scale data extraction without domestic value creation or regulatory control. India's localization framework reflects this shared concern, positioning data sovereignty as a corrective to

[81] Pritam Sen, *supra* note 69, at 1520.
[82] INSTITUTE OF INTERNATIONAL FINANCE, *Data Localization: Costs, Trade-offs, and Impacts Across the Economy* (Dec. 2020) https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf
[83] Erol Yayboke, *supra* note 54.
[84] Keyur Tripathi, *Data Localization and its Impact on Global Tech Companies Operating in India*, LAW COMMUNICANTS (June 29, 2025) https://thelawcommunicants.com/data-localization-and-its-impact-on-global-tech-companies-operating-in-india/?utm_source=chatgpt.com.
[85] *The Global Rise of Data Localization and Its Risks*, https://trustarc.com/resource/global-rise-data-localization-risks/ (last visited Feb. 30, 2026).

ISSN: 2582-6433

structural inequalities embedded in the global digital economy.

Policy assessments note that while localization carries risks including increased compliance complexity and potential market fragmentation, it also represents a strategic attempt by Global South states to reclaim jurisdictional authority over critical digital resources. [86] In this sense, India contributes to reshaping global norms by questioning the universality of liberal digital governance models.

India's approach, therefore, sits within a pluralistic global regime where varying localization and transfer policies reflect competing visions of sovereignty, economic strategy, and rights protection.[87] By prioritizing sovereign control and regulatory oversight, India directly challenges the normative dominance of free data flows. This shift underscores the fragmentation of international law governing data flows and signals a broader transformation in how sovereignty, security, and economic integration are negotiated in the digital age[88].

4. India's Sovereignty-Oriented Digital Engagement

India's participation in multilateral digital governance forums including the **WTO, G20, BRICS, and United Nations** has increasingly functioned as a "site of normative contestation" over the regulation of cross-border data flows. In these arenas, India has resisted the consolidation of a singular, trade-centric model of digital governance premised on the unrestricted movement of data.[89]

Instead, it has foregrounded concerns relating to regulatory sovereignty, developmental equity, and the uneven distribution of economic value in the global digital economy, particularly for developing states. Across "WTO e-commerce negotiations and G20 digital economy working groups", India has consistently argued that data governance frameworks must preserve domestic policy space. This highlights that India conceptualizes "data as a strategic national resource rather than merely a commercial asset", linking data governance to broader objectives of economic development, privacy protection, and national security. This approach reflects skepticism toward binding international commitments that could constrain a state's ability to regulate data flows in accordance with domestic constitutional and developmental priorities.[90]

Within BRICS platforms, India's position aligns closely with other Global South states seeking to recalibrate international digital norms. By advocating flexible, context-sensitive regulatory

[86] *Id.*
[87] *See, Data Localization*, *supra* note 45 at 3330.
[88] Keyur Tripathi, *supra* note 84.
[89] Anirudh Burman, *supra* note 3.
[90] Institute of International Finance, *supra* note 82.

ISSN: 2582-6433

models, India contributes to the emergence of a pluralistic digital order that recognizes differentiated capacities and historical inequalities. This positioning enables India to act as a Global South norm entrepreneur, shaping discourse around digital sovereignty and development while challenging the normative dominance of Global North–led free flow of data frameworks.[91] In doing so, India does not reject "global digital integration" but seeks to renegotiate its terms, embedding sovereignty and equity at the core of international digital law.

5. Implications for Global Data Governance

India's stance has broader implications for global governance. The proliferation of localization regimes contributes to internet fragmentation, where data is increasingly governed by territorial rules rather than global standards[92]. While fragmentation raises concerns about inefficiency and interoperability, it also reflects "the reality of regulatory pluralism" in a multipolar digital order.

At the level of international law, data localization highlights the fragmentation of international law governing data flows. Trade law, human rights law, cybersecurity norms, and domestic data protection frameworks often operate in tension, with no comprehensive global agreement on data governance. As each state defines its own conditions for data residency and transfer, businesses face mounting challenges in aligning their operations with competing regulatory demands, particularly where privacy protections and sovereignty imperatives diverge.[93] India's approach underscores the inadequacy of existing international frameworks to address competing sovereign claims over data.

Enforcing localization in "transnational digital environments" remains a significant challenge. Cloud infrastructure, platform dominance, and extraterritorial data processing complicate jurisdictional control. As localization grows, reconciling sovereign interests with the borderless nature of the internet will remain a central governance dilemma.

VI. Critiques and Counterarguments

Critics of data localization argue that the purported benefits come at significant economic and innovation costs. Localization mandates increase compliance burdens and infrastructure expenditures by forcing companies to duplicate storage and processing environments across

[91] *See*, *Data Localization*, *supra* note 45 at 3329.
[92] Institute of International Finance, *supra* note 82.
[93] Anirudh Burman, *supra* note 3.

ISSN: 2582-6433

jurisdictions[94].

Economists have found that such requirements can constrain trade, lower productivity, and raise costs for downstream industries, as the value of data is maximized when it moves seamlessly across borders for analytics, machine learning, and global services. Localization also "fragments data ecosystems and complicates compliance frameworks", particularly for smaller firms and startups with limited resources, thereby reducing competition and deterring investment.

Concerns extend beyond economics to governance and human rights. Storing data within national borders does not inherently guarantee privacy or security; it may increase the number of vulnerable endpoints and, without robust legal safeguards, expand opportunities for domestic surveillance. Proximity of data to state agencies can make it easier for governments to access or exploit personal information under broad legal authorizations, raising civil liberties concerns.

Moreover, localization may not sufficiently address the structural inequities of digital colonialism but could instead shift control from foreign to domestic actors without addressing underlying power imbalances.[95] To mitigate these risks, critics advocate proportionality-based approaches such as robust "privacy frameworks, international adequacy mechanisms, and privacy-preserving technologies" that balance sovereignty with interoperability rather than rigid localization mandates that can stifle innovation and entrench fragmentation.

VII. The Way Forward: Towards an Equitable Digital International Legal Order

An equitable digital international legal order must reconcile state claims to digital sovereignty with the inherently transnational nature of data flows. Rather than framing sovereignty and international cooperation as competing objectives, future governance models should enable "regulatory autonomy alongside interoperability" through mechanisms such as adequacy frameworks, mutual recognition, and multilateral safeguards grounded in shared minimum standards.

[94] Keyur Tripathi, *supra* note 84.
[95] Institute of International Finance, *supra* note 82.

ISSN: 2582-6433

Global South leadership is essential to this transformation. Developing states, which have historically borne the costs of "data extractivism and digital dependency", are well positioned to articulate alternative norms that prioritize developmental equity, regulatory flexibility, and public interest governance[96]. Coordinated Global South engagement can counter the dominance of Global North–centric models and reshape digital norm-setting processes.

Alongside institutional reform, alternative governance models are reshaping how sovereignty and interoperability can coexist. Privacy-preserving technologies such as federated learning, data trusts, confidential computing, and blockchain-based identity systems shift regulatory focus from the physical location of data to the conditions under which it is accessed and processed[97]. These approaches offer decentralized control without reinforcing digital silos, enabling innovation while mitigating compliance risks and sovereignty concerns.

Reform of international trade and data governance frameworks is equally necessary. Trade regimes must move beyond rigid commitments to free data flows and incorporate explicit protections for privacy, security, and developmental objectives.

Finally, sustainable digital governance must be rooted in constitutional and rights-based principles. "Embedding dignity, proportionality, transparency, and accountability ensures that digital sovereignty strengthens democratic governance rather than entrenching state or corporate power."

VIII. Conclusion

This paper has argued that data localization must be understood not merely as a regulatory or economic instrument, but as a legitimate assertion of digital sovereignty in response to contemporary forms of digital colonialism. In an international legal order historically shaped by Global North priorities and market-driven logics, "data localization represents an effort by states particularly in the Global South to reclaim jurisdictional authority over data generated within their territories". Far from being an inherently protectionist measure, localization emerges as a sovereign response to asymmetries in power, infrastructure, and value extraction that characterize the global digital economy.

[96] *See, Privacy Laws, supra* note 55.
[97] Erol Yayboke, *supra* note 54.

ISSN: 2582-6433

India's approach exemplifies this reorientation. Through its evolving data protection framework, sector-specific localization mandates, and strategic engagement in multilateral forums, India has sought to balance participation in global digital markets with the preservation of regulatory autonomy. In doing so, India positions itself as a norm entrepreneur in international law, actively contesting the dominance of the free flow of data doctrine and advancing alternative governance principles grounded in development, constitutional values, and public interest regulation. India's interventions in platforms such as the WTO, G20, BRICS, underscore its role in shaping a more pluralistic discourse on digital governance one that recognizes differentiated capacities and historical inequities.

At a broader level, the paper highlights the implications of data localization for decolonizing the digital international legal order. Digital colonialism operates through the concentration of data, platforms, and rule-making power in a handful of jurisdictions and corporations. Localisation, despite its imperfections, undermines this model by questioning the notion of data's remoteness and reaffirming the significance of territorial government in the digital era. However, the paper also recognizes the limits of localization as a resistance mechanism. Without robust safeguards, localization risks enabling state overreach, domestic surveillance, or the mere transfer of control from foreign to local elites without addressing deeper structural inequalities.

Reassessing sovereignty in the context of digital colonialism therefore requires a nuanced approach. Data localization should be viewed as a strategic but limited tool, capable of strengthening regulatory capacity and bargaining power, but insufficient on its own to achieve digital justice. Its effectiveness ultimately depends on complementary measures, including rights-based data governance, international cooperation, and the development of interoperable and privacy-preserving digital infrastructures.

Looking forward, India has the potential to play a transformative leadership role in fostering a more equitable international digital legal order. By advocating proportional, constitutionally grounded localization measures while promoting global standards based on trust, adequacy, and mutual respect, India can help bridge the divide between sovereignty and interoperability. In doing so, it can contribute to a future digital order that is not only globally connected, but also inclusive, accountable, and just.

ISSN: 2582-6433

Bibliography

Books

1. *Anupam Chander, The Electronic Silk Road: How the Web Binds the World Together in Commerce (Yale University Press, 2013).*
2. *Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press, 2013).*
3. *Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2014).*
4. *Paul M. Schwartz & Daniel J. Solove, Information Privacy Law (Aspen Publishers, 2018).*
5. *Mira Burri, Data Flows and Digital Trade in the Global Economy (Cambridge University Press, 2021).*
6. *Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019).*

Journal Articles

1. *Anupam Chander & Uyên P. Lê, "Data Nationalism," Emory Law Journal (2015).*
2. *Dan Jerker B. Svantesson, "Data Localization and the Future of Data Privacy," International Data Privacy Law (2017).*
3. *Rohit Chopra & Lina Khan, "The Case for Antitrust Against Big Tech," Yale Law Journal Forum (2020).*
4. *Arindrajit Basu, "Data Localization in India: Sovereignty, Security and Economic Development," Indian Journal of Law and Technology (2018).*
5. *Mira Burri, "The Governance of Data and Digital Trade," World Trade Review (2020).*
6. *Nikhil Pahwa, "Digital Sovereignty and Data Localization in India," Economic and Political Weekly (2019).*

Reports

1. *Government of India,* ***Justice B.N. Srikrishna Committee Report on Data Protection*** *(2018).*
2. *Ministry of Electronics and Information Technology (MeitY),* ***Report on Data Governance Framework Policy*** *(2022).*
3. *United Nations Conference on Trade and Development (UNCTAD),* ***Digital Economy Report*** *(2021).*
4. *World Economic Forum,* ***Data Free Flow with Trust Report*** *(2020).*

ISSN: 2582-6433

5. *Internet Freedom Foundation,* ***Data Localization and Digital Rights in India Report*** *(2021).*

Statutes and Legal Instruments

1. *Digital Personal Data Protection Act, 2023 (India).*
2. *Information Technology Act, 2000 (India).*
3. *General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.*
4. *Draft Personal Data Protection Bill, 2019 (India).*

Case Laws

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.*
2. *Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.*
3. *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*