INDIAN JOURNAL OF JURISPRUDENCE AND REVIEWS (IJJR)
(Open Access, Double-Blind Peer Reviewed Journal)
ISSN Online: ISSN Print

Cross-Border Data Flows and Digital Trade: Challenges For Indian Law

Malavika J

Assistant Professor, Kerala Law College, Kerala University, Kerala, India.

Article information

Received: 5th December 2025
Received in revised form: 7th January 2026
Accepted: 9th February 2026
Available online: 2nd March 2026

Volume: 2
Issue: 1
DOI: https://doi.org/10.5281/zenodo.18831756

Abstract

The proliferation of cross-border data flows has become integral to digital trade, yet poses significant regulatory challenges for Indian privacy and competition law frameworks. This paper examines the legal complexities arising from the intersection of data localization requirements under the Digital Personal Data Protection Act, 2023, and competition concerns regarding market dominance by Big Tech platforms. Through analysis of recent Competition Commission of India orders and evolving jurisprudence, this paper identifies critical tensions between data sovereignty imperatives and international trade obligations. The study demonstrates that India's current regulatory approach, while protective of domestic interests, may inadvertently create barriers to digital trade and innovation. This paper proposes a balanced framework that harmonizes privacy protection, competition enforcement, and trade facilitation through risk-based data governance mechanisms. The findings suggest that India must adopt internationally interoperable standards while preserving regulatory autonomy to effectively participate in the global digital economy.

Keywords: - Cross-border data flows, Data localization, Digital trade, Market dominance, Competition law

I. INTRODUCTION

Cross-border data flows have emerged as the lifeblood of the contemporary digital economy, facilitating global supply chains, cloud computing services, and international e-commerce transactions valued at trillions of dollars annually (Meltzer, 2019). For India, with its burgeoning digital economy projected to reach $1 trillion by 2025, seamless data flows are critical for economic growth and technological advancement (MEITY, 2023). However, the unrestricted movement of personal and non-personal data across jurisdictions raises profound concerns regarding national sovereignty, individual privacy rights, and competitive market dynamics.

India's regulatory response has been characterized by a dual emphasis on data protection and competition enforcement. The Digital Personal Data Protection Act (DPDPA), 2023, represents India's most comprehensive attempt to regulate personal data processing, incorporating elements of both the European Union's General Data Protection Regulation and indigenous privacy principles derived from the Supreme Court's landmark *Puttaswamy* decision (Puttaswamy v. Union of India, 2017). Simultaneously, the Competition Commission of India (CCI) has increasingly scrutinized Big Tech platforms for allegedly leveraging data advantages to entrench market dominance and exclude competitors (CCI v. Google LLC, 2022).

This regulatory landscape creates inherent tensions. Data localization mandates, justified on privacy and security grounds, may conflict with international trade commitments under the World Trade Organization's General Agreement on Trade in Services (GATS) and bilateral agreements (Chander & Lê, 2015). Competition interventions targeting data-driven network effects may inadvertently discourage cross-border data sharing essential for artificial intelligence development and other innovations. These contradictions necessitate a systematic examination of how Indian law can reconcile competing imperatives.

This paper addresses three central questions:

- First, how do data localization requirements under Indian privacy law affect digital trade flows and international commerce?

- Second, what are the competition law implications of cross-border data transfers by dominant digital platforms?
- Third, what legal framework can harmonize privacy protection, competition enforcement, and trade facilitation?

Through doctrinal analysis supplemented by comparative perspectives, this paper proposes a balanced regulatory approach.

II. LEGAL AND REGULATORY FRAMEWORK

India's regulation of cross-border data flows operates through multiple, sometimes overlapping, legal instruments. The DPDPA, 2023, establishes the foundational framework for personal data protection, while sector-specific regulations impose additional constraints. The Competition Act, 2002, as amended, provides the CCI with broad powers to investigate anti-competitive practices involving data (Ministry of Law and Justice, 2023).

The DPDPA adopts a consent-based model for cross-border data transfers, requiring data fiduciaries to obtain explicit consent from data principals before transferring personal data to jurisdictions outside India (Section 16, DPDPA, 2023). This provision grants the Central Government authority to notify 'restricted countries' to which data transfers are prohibited, creating uncertainty for businesses engaged in international operations. The Act further mandates certain categories of data fiduciaries to maintain copies of personal data within Indian territory, though the specific categories remain subject to executive notification.

From a competition law perspective, the CCI has established that data constitutes a valuable economic asset and competitive advantage. In its investigation of Google's practices in the Android ecosystem, the CCI found that user data collected through bundled applications created significant barriers to entry, as competing platforms could not replicate the data advantages accumulated over time (CCI v. Google LLC, 2022). This jurisprudence signals that cross-border data flows by dominant entities may face heightened scrutiny where such flows reinforce market power.

India's international trade commitments present additional complexity. Under GATS Article XIV, India may adopt measures necessary to protect privacy, provided such measures are not arbitrary discrimination or disguised trade restrictions (Burri, 2017). The Regional Comprehensive Economic Partnership, which India declined to join, includes provisions on cross-border data flows that would have constrained data localization measures. India's current negotiating position in bilateral trade agreements emphasizes regulatory flexibility while resisting binding commitments on data flows (Ministry of Commerce, 2023).

III. CROSS-BORDER DATA FLOWS: PRIVACY AND TRADE TENSIONS

Data localization requirements, while ostensibly protective of privacy and national security, create substantial friction in digital trade. Empirical studies estimate that mandatory data localization reduces GDP by 0.7 to 1.7 percent in implementing countries, primarily through increased operational costs for businesses and reduced economies of scale (Bauer et al., 2016). For India, where digital services exports exceeded $194 billion in 2022, these costs are significant.

The DPDPA's approach differs materially from the GDPR's adequacy framework. While the GDPR permits data transfers to jurisdictions deemed to provide adequate protection through European Commission decisions, India's notification-based restriction mechanism lacks clear standards or procedural safeguards (Greenleaf, 2024). This unpredictability deters foreign investment and complicates compliance for multinational corporations. Indian IT services firms, which rely on cross-border data flows to deliver services globally, have expressed concerns that reciprocal restrictions by trading partners could harm their competitive position.

Moreover, the efficacy of data localization in protecting privacy remains contested. Localization may enhance government access to data for surveillance purposes while doing little to prevent breaches or misuse by private actors (Selby, 2017). The Supreme Court in *Puttaswamy* emphasized proportionality in privacy restrictions, suggesting that blanket localization mandates may not satisfy constitutional scrutiny absent demonstrable necessity (Puttaswamy v. Union of India, 2017).

The legal uncertainty is compounded by the absence of implementing rules under the DPDPA. Critical issues including the definition of 'restricted countries,' specific data categories subject to localization, and exemptions for intra-group transfers remain unresolved. This regulatory vacuum forces businesses to adopt overly conservative compliance strategies, potentially foregoing beneficial cross-border collaborations (Kazim et al., 2023).

IV. COMPETITION LAW DIMENSIONS OF DATA FLOWS

The competition law analysis of cross-border data flows involves two distinct concerns: exclusionary conduct by dominant platforms and merger control in data-driven markets. The CCI's orders in Google Android and WhatsApp demonstrate evolving enforcement priorities (CCI v. Meta Platforms, 2023).

In the Google Android matter, the CCI found that Google leveraged its dominant position in app stores to impose requirements that app developers share user data, which Google then utilized across its ecosystem to strengthen network effects. The Commission held that such data aggregation practices constitute abuse under Section 4 of the Competition Act, particularly where they create barriers to market entry (CCI v. Google LLC, 2022). This precedent implies that cross-border data transfers facilitating such aggregation may face regulatory challenge.

The proposed amendments to the Competition Act introduce ex-ante regulations for 'Systemically Important Digital Enterprises' (SIDEs), which would restrict certain data practices including data portability limitations and interoperability refusals (Competition Amendment Bill, 2023). These provisions, inspired by the EU Digital Markets Act, could significantly affect how global platforms structure their data flows involving Indian users.

However, competition intervention in data markets presents analytical challenges. The traditional framework of defining relevant markets and assessing market power based on price effects fits poorly with zero-price digital services where

data serves as consideration (Ohlhausen & Okuliar, 2015). The CCI has begun to develop methodologies accounting for quality degradation, innovation suppression, and attention markets, but jurisprudence remains nascent (Poddar & Ghosh, 2023).

A further complication arises from the tension between competition enforcement and data protection. Remedies such as mandatory data sharing, intended to reduce entry barriers, may conflict with privacy principles limiting data processing and transfers. The CCI has acknowledged this tension but has not articulated clear principles for balancing competing values (CCI, 2024). International coordination mechanisms remain underdeveloped, creating risks of contradictory enforcement outcomes.

V. CRITICAL EVALUATION: SHORTCOMINGS AND CONTRADICTIONS

India's current approach to cross-border data governance suffers from three fundamental deficiencies: regulatory fragmentation, inadequate international coordination, and insufficient empirical grounding.

First, the multiplicity of regulatory frameworks creates compliance complexity and legal uncertainty. The Reserve Bank of India's data localization directive for payment systems, the Insurance Regulatory and Development Authority's requirements for insurance data, and the DPDPA's general framework operate independently without clear harmonization mechanisms (RBI, 2018). This sectoral fragmentation contradicts principles of regulatory coherence and proportionality.

Second, India's limited participation in international data governance initiatives isolates it from emerging global standards. The Cross-Border Privacy Rules system under APEC, the OECD Privacy Guidelines, and bilateral adequacy arrangements operate largely without Indian engagement. This isolation may prove counterproductive as trading partners increasingly condition market access on demonstrable data protection standards (Casalini & López González, 2019). The absence of bilateral mechanisms with major partners like the European Union and United States creates uncertainty for cross-border commerce.

Third, policy formulation has proceeded without adequate empirical assessment of costs and benefits. No comprehensive study has evaluated whether data localization measurably improves security outcomes or whether alternative measures such as encryption and breach notification could achieve similar objectives at lower economic cost. Similarly, competition interventions targeting data practices lack rigorous counterfactual analysis of effects on innovation and consumer welfare. Evidence-based policymaking requires systematic collection and analysis of market data, which remains inadequate in the Indian context.

VI. IMPLICATIONS AND RECOMMENDATIONS

Addressing these challenges requires a multi-dimensional reform agenda encompassing regulatory harmonization, international engagement, and institutional capacity building.

First, India should adopt a risk-based approach to data governance that calibrates restrictions to demonstrable harms rather than categorical prohibitions. This framework, advocated by international best practices, would classify data based on sensitivity and impose proportionate controls (UNCTAD, 2021). For instance, anonymized or aggregated data used for business analytics might flow freely, while biometric or health data could face stricter requirements. Such differentiation would reduce compliance costs while preserving protection for genuinely sensitive information.

Second, regulatory coordination mechanisms should be strengthened through establishment of an inter-ministerial body with authority to harmonize data governance policies across sectors. This body could develop unified standards for cross-border transfers, resolve conflicts between privacy and competition objectives, and ensure alignment with international commitments. The model of Australia's Consumer Data Right framework, which integrates privacy protection with competition-enhancing data portability, offers valuable lessons (Treasury of Australia, 2019).

Third, India should pursue strategic engagement with international data governance initiatives. Negotiating adequacy arrangements with the European Union would facilitate data flows with India's largest services export market. Participation in APEC's Cross-Border Privacy Rules system would demonstrate commitment to international standards while preserving domestic regulatory authority. These engagements need not require wholesale adoption of foreign frameworks but rather mutual recognition of substantially equivalent protections.

Fourth, competition law enforcement should develop data-specific analytical frameworks that account for multi-sided markets, network effects, and innovation dynamics. The CCI's proposed Digital Markets Unit should collaborate with international counterparts to develop common methodologies and coordinate investigations of global platforms. Regulatory sandboxes could enable controlled experimentation with data sharing remedies to assess effectiveness before widespread implementation.

VII. CONCLUSION

Cross-border data flows present India with a fundamental policy dilemma: how to protect legitimate interests in privacy and competition while enabling participation in the global digital economy. The current regulatory framework, characterized by data localization mandates and emerging competition interventions, reflects a cautious approach prioritizing sovereignty and control. However, this caution carries substantial costs in foregone economic growth, reduced innovation, and international isolation.

This paper has demonstrated that the tensions between privacy protection, competition enforcement, and trade facilitation are not insurmountable. A risk-based regulatory framework that differentiates data based on sensitivity, coupled with robust institutional coordination and strategic international engagement, can reconcile competing objectives. Such an approach would align with constitutional principles of proportionality established in *Puttaswamy* while positioning India as a credible rule-maker in global digital governance.

The path forward requires political will to resist protectionist pressures and embrace evidence-based policymaking. India's digital economy stakeholders from technology firms to civil society organizations must engage constructively in

shaping balanced regulations. International partners, particularly the European Union and United States, can facilitate this process through technical assistance and mutual recognition frameworks.

Future research should focus on empirical assessment of data governance policies' effects on innovation, investment, and welfare outcomes. Comparative analysis of different regulatory models, from the EU's rights-based approach to Singapore's business-friendly framework, can inform Indian policy development. As artificial intelligence and emerging technologies increase data's economic salience, the need for coherent cross-border data governance will only intensify. India's choices today will shape its digital future for decades to come.

REFERENCES

Bauer, M., Ferracane, M. F., Kren, J., & van der Marel, E. (2016). *Tracing the economic impact of regulations on the free flow of data and data localization* (ECIPE Occasional Paper No. 2/2016). European Centre for International Political Economy.

Burri, M. (2017). The regulation of data flows through trade agreements. *Georgetown Journal of International Law, 48*(2), 407–448.

Casalini, F., & López González, J. (2019). *Trade and cross-border data flows* (OECD Trade Policy Papers No. 220). OECD Publishing.

CCI v. Google LLC, Case No. 07 of 2020 (Competition Commission of India 2022).

CCI v. Meta Platforms Inc., Case No. 13 of 2022 (Competition Commission of India 2023).

Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal, 64*(3), 677–739.

Competition Commission of India. (2024). *Market study on e-commerce in India*. CCI Market Studies Unit.

Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code.

Greenleaf, G. (2024). India's 2023 data protection act: Privacy setback or strategic evolution? *Computer Law & Security Review, 52*, 105932.

Kazim, E., Denny, D. M., & Koshiyama, A. (2023). AI auditing and impact assessments: Towards a framework for digital regulation in India. *Computer Law & Security Review, 48*, 105790.

Meltzer, J. P. (2019). Governing digital trade. *World Trade Review, 18*(S1), S23–S48.

Ministry of Commerce and Industry. (2023). *India's approach to digital trade negotiations*. Department of Commerce.

Ministry of Electronics and Information Technology. (2023). *India's trillion-dollar digital economy vision*. Government of India.

Ministry of Law and Justice. (2023). *The Competition (Amendment) Bill, 2023* (Bill No. 131 of 2023). Government of India.

Ohlhausen, M. K., & Okuliar, A. P. (2015). Competition, consumer protection, and the right (approach) to privacy. *Antitrust Law Journal, 80*(1), 121–156.

Poddar, P., & Ghosh, S. (2023). Competition law and digital platforms in India: Emerging jurisprudence. *Journal of Antitrust Enforcement, 11*(2), 234–259.

Puttaswamy v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

Reserve Bank of India. (2018). *Storage of payment system data* (RBI Circular No. RBI/2017-18/153).

Selby, J. (2017). Data localization laws: Trade barriers or legitimate responses to cybersecurity risks? *International Journal of Law and Information Technology, 25*(3), 213–232.

Treasury of Australia. (2019). *Consumer data right: Overview*. Australian Government Treasury.

United Nations Conference on Trade and Development. (2021). *Data protection and privacy legislation worldwide* (UNCTAD Policy Brief No. 109).