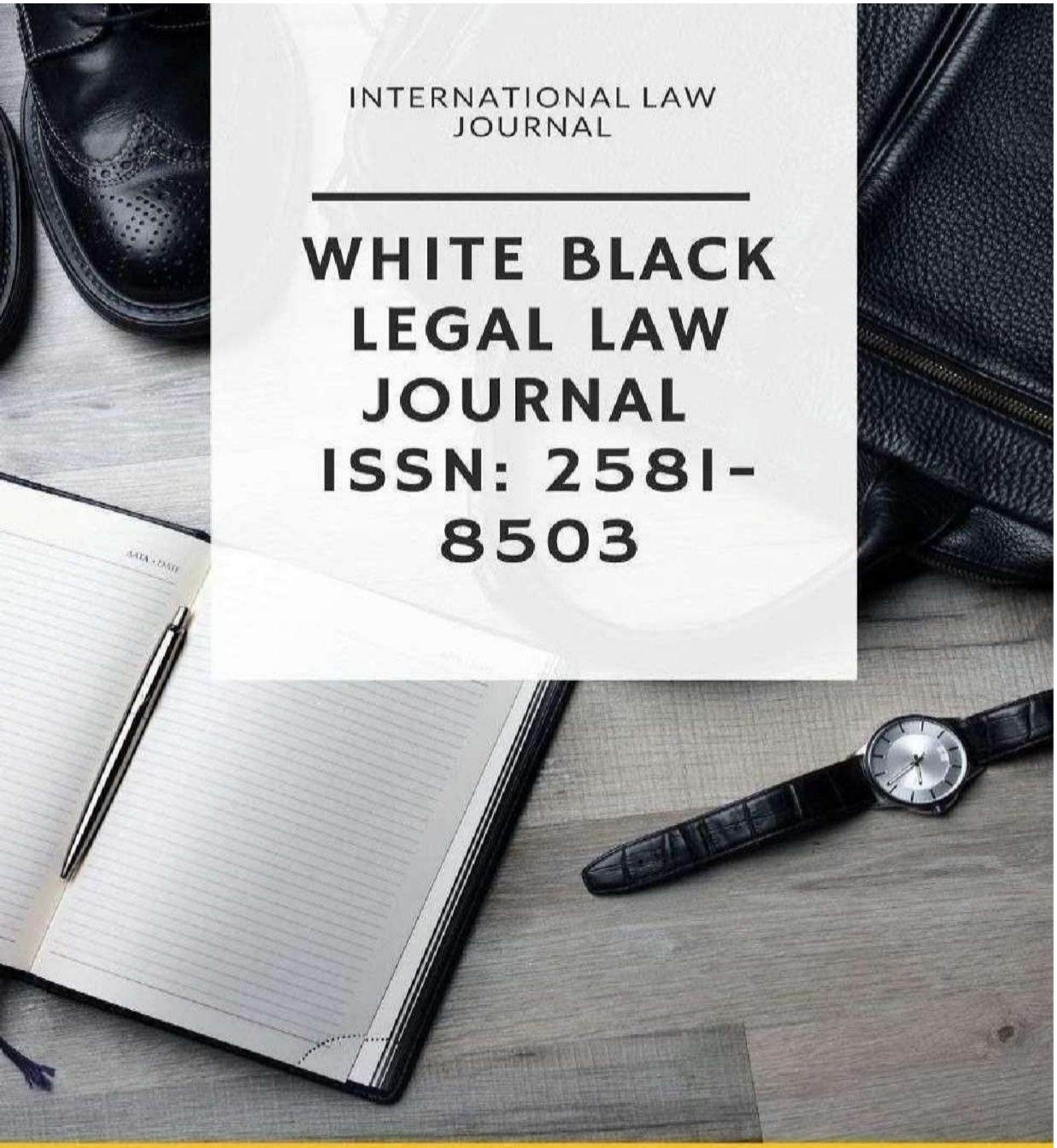

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CROSS-BORDER FINANCIAL DATA TRANSFERS IN INDIA: CONSTITUTIONAL FOUNDATIONS, REGULATORY INTERPLAY BETWEEN THE DPDP ACT, 2023 AND RBI REGULATIONS, AND THE EMERGING GOVERNANCE FRAMEWORK

AUTHORED BY - RICHA KUMARI
BBA. LLB(H), (Corporate law),
Amity Law School, Amity University, Noida

Abstract

The rapid digitization of financial systems has transformed how economies generate, process, and transmit data across jurisdictions. India, now home to one of the world's largest digital financial ecosystems, has responded to this transformation with two overlapping regulatory instruments: The Digital Personal Data Protection Act, 2023 (DPDP Act) and the sectoral directives of the Reserve Bank of India (RBI). This article undertakes a comprehensive examination of the constitutional foundations of data privacy in India, the legislative journey from the fragmented pre-DPDP era to the present codified regime, and the practical implications of the dual-regulatory framework for financial institutions engaged in cross-border data transfers. Drawing on case studies involving multinational payment platforms and a comparative review of international data protection models, the article argues that India has constructed a hybrid governance architecture—one that combines the consent-driven flexibility of the DPDP Act with the sovereignty-oriented rigidity of RBI localization mandates. While this architecture represents a significant advancement, substantial normative gaps, ambiguous compliance obligations, and institutional design concerns continue to undermine its efficacy. The article concludes by identifying areas that demand legislative clarification and regulatory coordination.

Keywords: *Digital Personal Data Protection Act 2023, RBI data localization, cross-border financial data, data sovereignty, fintech regulation, GDPR comparison, Puttaswamy judgment, Payment Systems Act.*

1. Introduction

The movement of financial data across national boundaries is no longer a peripheral concern of Tele communications policy—it sits at the very core of contemporary economic governance. As financial institutions, payment aggregators, and technology platforms increasingly operate across multiple jurisdictions, the question of which laws govern the collection, storage, and transfer of personal financial data has acquired profound regulatory, constitutional, and commercial dimensions. India, with its extraordinary digital growth trajectory, offers a particularly instructive case study in how emerging economies negotiate the tensions between open data flows, national sovereignty, and individual privacy.

India's digital economy has expanded at a pace that few could have predicted even a decade ago. With over 850 million internet users, a Unified Payments Interface that processes billions of transactions monthly, and a fintech sector that attracted billions in foreign investment, the country now generates and transmits financial data at a scale that rivals established digital economies. By 2025, the total value of data-driven cross-border financial flows involving Indian entities exceeded one trillion US dollars annually. This figure reflects not only the scale of opportunity but also the magnitude of regulatory responsibility.

Yet until 2023, India lacked a comprehensive statute governing the protection of personal data. Financial information—encompassing transaction histories, account identifiers, PAN numbers, and credit records—was protected only by a patchwork of provisions in the Information Technology Act, 2000 and subordinate rules promulgated in 2011. The inadequacy of this framework became increasingly apparent as data breaches multiplied, foreign regulators questioned the adequacy of Indian data protections, and the Supreme Court declared privacy a fundamental right in its landmark 2017 ruling.

The enactment of the Digital Personal Data Protection Act in August 2023 marked a decisive inflection point. For the first time, India possessed a dedicated statutory framework for the protection of digital personal data, including financial data. The Act introduced a consent-based processing model, established the Data Protection Board of India, and adopted a nuanced approach to cross-border data transfers through a negative-list or blacklist mechanism. Simultaneously, the Reserve Bank of India continued to enforce its own, considerably stricter data localization regime, creating a dual-layered compliance architecture that financial institutions must navigate.

This article examines that architecture systematically. Part 2 traces the constitutional underpinnings of data protection in India, culminating in the Puttaswamy judgment of 2017.

Part 3 surveys the pre-DPDP regulatory landscape, including the IT Act provisions and the Sensitive Personal Data or Information Rules, 2011. Parts 4 and 5 analyses the DPDP Act in detail, focusing on its scope, key concepts, cross-border transfer provisions, and the implementation rules of 2025. Part 6 examines RBI's sector-specific regulations, including the 2018 localization mandate and subsequent directives. Part 7 explores the intersection and tensions between the two frameworks through selected case studies. Part 8 situates India's approach in a comparative global context. Part 9 offers a critical assessment of the framework's strengths and limitations. Part 10 concludes.

2. Constitutional Foundations: Privacy as a Fundamental Right

Any rigorous analysis of India's data protection regime must begin with the Constitution, for the legal legitimacy of the entire framework ultimately depends on the constitutional status of informational privacy. That status was, for many decades, deeply uncertain.

Early constitutional jurisprudence took a narrow approach. In M.P. Sharma v. Satish Chandra (1954), an eight-judge bench held that the Indian Constitution did not confer a fundamental right to privacy comparable to the Fourth Amendment in the United States. Eight years later, in Kharak Singh v. State of U.P. (1962), a six-judge bench reiterated that there was no explicit right to privacy in the Constitution, though a minority view dissented. These early pronouncements created a constitutional vacuum that would persist for decades.

The first meaningful judicial shift occurred in R.C. Cooper v. Union of India (1970), where the Supreme Court articulated that fundamental rights must be interpreted as an integrated whole rather than in isolation—a principle that would later provide doctrinal support for deriving unremunerated rights from Article 21's guarantee of life and personal liberty.

Subsequent decisions in Govind v. State of Madhya Pradesh (1975) and Rajgopal v. State of Tamil Nadu (1994) acknowledged a qualified right to privacy without fully resolving its constitutional status.

The decisive moment arrived with Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). A nine-judge Constitution Bench, convened to settle the question once and for all, unanimously declared that the right to privacy is a fundamental right intrinsic to Articles 14, 19, and 21 of the Constitution. The judgment is architecturally significant for data protection law in several respects. First, it recognized informational privacy—the individual's right to control the collection, use, and dissemination of personal data—as a dimension of the constitutionally protected right. Second, Justice D.Y. Chandrachud's concurring opinion elaborated on privacy

as essential to human dignity, autonomy, and the capacity for self-determination. Third, the Court established that privacy, though fundamental, is not absolute; any state interference must be authorized by law, must pursue a legitimate state aim, and must be proportionate to that aim. This tripartite test—legality, legitimate aim, and proportionality—has become the constitutional lens through which India's data protection legislation must be evaluated. The DPDP Act, the RBI's localization directives, and the government's power to restrict cross-border data transfers must all satisfy this standard. The Puttaswamy judgment thus does not merely provide a historical backdrop; it supplies the normative vocabulary within which India's entire data governance architecture must be understood and scrutinized.

3. The Pre-DPDP Regulatory Landscape

3.1 The Information Technology Act, 2000

Prior to the DPDP Act, the primary legislative instrument governing data in India was the Information Technology Act, 2000, supplemented by rules enacted under it. The IT Act was conceived primarily to facilitate electronic commerce and combat cybercrime; data protection was an incidental rather than a principal concern.

Section 43A of the IT Act, introduced by the 2008 amendment, imposed civil liability on body corporates that negligently handled sensitive personal data. Section 72 criminalized the breach of confidentiality and privacy by persons authorized to access electronic records. Section 72A extended liability to intermediaries who disclosed personal information in breach of a lawful contract. While these provisions offered some recourse to affected individuals, they were reactive, enforcement was weak, and the framework lacked systemic regulatory oversight.

3.2 The SPDI Rules, 2011

The Sensitive Personal Data or Information Rules, 2011, promulgated under Section 43A, represented the most substantive pre-DPDP attempt to regulate personal data. The Rules defined sensitive personal data to include financial information such as bank account details, credit and debit card numbers, and transaction histories, along with passwords, health data, and biometric information. They required organizations to publish privacy policies, to obtain prior consent before collecting sensitive data, to allow individuals to withdraw consent, and to maintain reasonable security practices.

Crucially, Rule 7 addressed cross-border data transfers, permitting them where the receiving entity ensured equivalent protection, the individual had consented, or the transfer was

necessary for contractual performance. This was India's first regulatory attempt to govern international data flows.

However, the SPDI Rules had significant structural weaknesses. They applied exclusively to private sector companies. Government agencies were entirely exempt. There was no independent data protection authority; enforcement relied on aggrieved individuals initiating civil proceedings. The Rules made no provision for data portability, data breach notification, or the accountability of data processors. As India's digital economy expanded exponentially over the following decade, these limitations became increasingly untenable. The absence of a unified legal framework not only exposed Indian citizens to data risks but also created reputational and legal uncertainty for businesses seeking to operate across jurisdictions.

4. The Digital Personal Data Protection Act, 2023: Architecture and Key Provisions

4.1 Legislative Journey

The DPDP Act is the product of nearly a decade of legislative deliberation. Following the Puttaswamy judgment, the Government constituted an expert committee chaired by Justice B.N. Srikrishna, whose 2018 report proposed a comprehensive data protection framework drawing on international models, particularly the EU's General Data Protection Regulation. The Personal Data Protection Bill, 2019 was introduced in Parliament but attracted substantial criticism: its data localization provisions were seen as excessively burdensome, its exemptions for government agencies were considered overly broad, and concerns were raised about the independence of the proposed Data Protection Authority. After a lengthy review by a Joint Parliamentary Committee, the government withdrew the Bill in 2022 and introduced a revised draft. The final Act was passed in August 2023, with implementing rules notified in November 2025. Full implementation is anticipated by May 2027.

4.2 Scope and Territorial Application

The DPDP Act applies to the processing of digital personal data within India, as well as to processing outside India when it relates to profiling or offering goods and services to individuals located within the country. This extraterritorial reach, modelled on the GDPR's Article 3, ensures that foreign entities handling Indian consumers' financial data are subject to the same regulatory obligations as domestic entities, preventing regulatory arbitrage. The Act defines personal data broadly as any data about an identifiable individual, and financial data—

including transaction records, account details, and identification numbers—falls squarely within this definition.

One notable departure from international practice is the Act's decision not to create a separate category of sensitive personal data. Under the GDPR, special categories of data attract heightened protection. The DPDP Act instead imposes stricter obligations on Significant Data Fiduciaries, a designation based on the volume and sensitivity of the data processed, the risk to individual rights, and potential impact on national security. Banks, large payment processors, and major fintech platforms are expected to be designated as Significant Data Fiduciaries.

4.3 The Consent Framework

The Act is fundamentally consent-driven. Personal data may be processed only if the data principal—the individual to whom the data relates—has given free, specific, informed, and unambiguous consent, or if processing falls within one of the specified legitimate uses. These legitimate uses include employment-related processing, processing necessary for the provision of services the individual has actively sought, and processing required by law. In the financial context, this means that banks and payment service providers must obtain meaningful consent for data collection and must ensure that consent is not bundled with terms and conditions in a manner that obscures its scope.

Data principals retain the right to withdraw consent at any time, though the Act acknowledges that withdrawal does not affect the legality of processing that occurred before withdrawal. This provision has significant practical implications for financial institutions that maintain long-term customer relationships based on data accumulated over years.

4.4 Obligations of Data Fiduciaries and the Data Protection Board

The Act imposes a suite of accountability obligations on data fiduciaries. They must provide clear and accessible notice to data principals at the time of data collection, specifying the purposes of processing and the rights available to individuals. They must ensure the accuracy of personal data, implement appropriate technical and organizational security safeguards, and report breaches to the Data Protection Board of India and affected data principals within prescribed timelines. Significant Data Fiduciaries face additional obligations, including the appointment of a Data Protection Officer, the conduct of Data Protection Impact Assessments before undertaking high-risk processing activities, and the engagement of independent data auditors.

The Data Protection Board, established under the Act as an independent adjudicatory body, is empowered to investigate complaints, issue orders, and impose penalties of up to rupees two hundred and fifty crore for serious violations. While this penalty regime represents a significant departure from the nominal civil liability under the IT Act, questions have been raised about the Board's institutional independence given that its members are appointed by the central government.

5. Cross-Border Data Transfers Under the DPDP Framework

5.1 The Blacklist Model and Its Implications

Section 16 of the DPDP Act governs cross-border transfers through a default-permissive or blacklist model: transfers of personal data to foreign countries are generally permitted unless the central government specifically restricts transfers to a particular country or territory through a notification. This approach represents a deliberate policy choice to priorities business flexibility and India's engagement with the global digital economy over stricter adequacy-based gate-keeping.

The model contrasts sharply with the EU's adequacy framework under the GDPR, which prohibits data exports to third countries unless the European Commission has determined that the destination country provides an adequate level of data protection, or unless specific transfer mechanisms such as Standard Contractual Clauses or Binding Corporate Rules are in place. China's Personal Information Protection Law, by contrast, requires a security assessment by the government before certain cross-border transfers can occur. India's approach, by design, is considerably more permissive, though the government retains the power to restrict transfers to particular jurisdictions if national security or public interest so requires.

As of April 2026, the government has not published a list of restricted countries. This absence of a blacklist creates a peculiar form of regulatory uncertainty: organizations technically face no restrictions on cross-border transfers under the DPDP Act, yet they remain in a state of anticipatory compliance, uncertain about which jurisdictions might be restricted and when. This uncertainty is particularly acute for financial institutions with global data supply chains.

5.2 The 2025 Rules and Contract-Based Safeguards

The Digital Personal Data Protection Rules, notified in November 2025, provide operational guidance on cross-border transfers. In the absence of adequacy determinations or standardized transfer mechanisms, the Rules rely heavily on contractual frameworks. Data fiduciaries that

transfer personal data to foreign processors or sub-processors must ensure that transfer agreements incorporate security standards equivalent to those required under the Act, breach notification obligations, audit rights, and data return or deletion obligations upon termination of the processing relationship. For Significant Data Fiduciaries, additional restrictions apply to the sharing of data with foreign entities that are state-controlled, reflecting the government's concerns about foreign governmental access to Indian citizens' data.

6. RBI Regulations: Sector-Specific Financial Data Governance

6.1 The 2018 Data Localization Circular

The Reserve Bank of India's approach to financial data governance predates the DPDP Act by several years and is considerably more prescriptive. On 6 April 2018, the RBI issued a circular under the Payment and Settlement Systems Act, 2007, requiring all payment system operators to ensure that the entire data relating to payment systems operated by them, including full end-to-end transaction data and information collected, carried, and processed as part of message or payment instruction, be stored only in India. Foreign storage was categorically prohibited. For cross-border transactions, the data may be processed abroad for completing the transaction, but must be deleted from foreign systems and returned to India within 24 hours.

The 2018 circular represented one of the most stringent data localization requirements globally and triggered considerable controversy. Major international payment platforms—including Visa, MasterCard, American Express, and PayPal—were required to restructure their data architectures, build or lease domestic server infrastructure, and demonstrate compliance through audits. The RBI's position was that localization was necessary to ensure that Indian payment data remained accessible to regulatory and law enforcement authorities without reliance on mutual legal assistance treaties or foreign judicial processes.

6.2 Payment Aggregator – Cross-Border Framework, 2023

In 2023, the RBI introduced a dedicated regulatory framework for cross-border payment aggregators—entities that facilitate international transactions for Indian merchants and consumers. The framework requires non-bank payment aggregators to obtain specific authorization from the RBI, to meet minimum net worth requirements, and to comply with reinforced data localization obligations. Banks holding Authorized Dealer Category-I licenses are exempt from certain requirements under this framework, reflecting a differentiated regulatory treatment premised on the existing supervisory oversight to which banks are subject.

6.3 IT Outsourcing Master Direction, 2023

The RBI's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023, governs how regulated entities may outsource IT services and cloud computing. The Direction requires that data hosted in cloud environments be stored on infrastructure physically located in India, with appropriate data segregation and access controls. Financial institutions must conduct due diligence on cloud service providers, retain audit rights, and ensure that contractual arrangements allow the RBI to access data and conduct inspections. Cyber incidents must be reported to the RBI within prescribed timeframes.

6.4 The Indian Financial System Cloud

Looking ahead, the RBI has proposed the development of a dedicated Indian Financial System Cloud—a sovereign, government-facilitated cloud infrastructure designed specifically for the financial sector. This initiative reflects the RBI's broader philosophy that financial data constitutes a national asset that must be protected not only through legal regulation but through the creation of domestic technological infrastructure. The proposal, if implemented, would significantly enhance India's capacity to enforce localization requirements and reduce the dependency of financial institutions on foreign cloud providers.

7. Compliance in Practice: Illustrative Case Studies

The abstract regulatory framework described above acquires meaning in the context of actual compliance experiences. The following cases illustrate how financial institutions and technology platforms have navigated—or failed to navigate—India's data governance requirements.

7.1 WhatsApp Payments

WhatsApp's attempt to launch its UPI-based payment service in India provides one of the most extensively documented examples of regulatory compliance with RBI localization requirements. After a pilot in 2018, the RBI imposed compliance conditions before permitting full-scale operation. The company was required to localize all payment data within India, build domestic data infrastructure, appoint a nodal officer to liaise with Indian regulators, and file an audit report confirming compliance. The matter reached the Supreme Court of India, where WhatsApp submitted affidavits confirming compliance. Full operational approval was eventually granted in 2020 only after these conditions were satisfied. The case demonstrates

that even entities of significant global market power are not exempt from India's localization requirements and that judicial oversight plays a role in ensuring regulatory accountability.

7.2 Amazon Pay

Amazon Pay's experience in India illustrates the feasibility of a hybrid compliance model. Faced with the RBI's localization requirements, Amazon restructured its payment data architecture, shifting the storage of Indian payment transaction data to servers located in Mumbai. Global analytics and non-payment data continued to flow through Amazon's international infrastructure under conditional approvals. The Amazon case is instructive because it demonstrates that compliance with strict localization requirements does not necessarily require the complete decoupling of Indian operations from global technology infrastructure; rather, it demands careful data classification and architectural segmentation.

7.3 Google Pay

Google Pay faced legal scrutiny in India following allegations that payment data was being stored on servers outside the country. The litigation and subsequent regulatory proceedings reinforced a principle that is now well established in Indian regulatory practice: localization obligations attach to the data itself, regardless of the corporate structure or nationality of the entity involved. The requirement is agnostic to whether the entity is a domestic startup or a subsidiary of a multinational corporation.

7.4 Ant Financial

Perhaps the most instructive case from a market access perspective is the exit of Ant Financial—the financial services affiliate of China's Alibaba Group—from the Indian market. Following regulatory scrutiny in the context of broader geopolitical concerns about Chinese investment in Indian digital infrastructure, and in the face of stringent data localization requirements, Ant Financial divested its stakes in Indian fintech ventures and withdrew from the market. The case illustrates that non-compliance, or the commercial unviability of compliance, can result in complete market exclusion, underscoring the seriousness with which India's regulators approach data sovereignty in the financial sector.

8. A Comparative Perspective

India's regulatory architecture for cross-border financial data can be situated within a broader global landscape of data governance models, each reflecting different conceptions of the

relationship between state authority, market freedom, and individual rights.

The European Union's approach under the General Data Protection Regulation is premised on the concept of data protection as a fundamental right, with cross-border transfers permitted only to countries that offer equivalent protection or through specific legal mechanisms such as Standard Contractual Clauses, Binding Corporate Rules, or derogations. The EU model prioritizes individual rights and mutual recognition between jurisdictions. Its adequacy determinations serve as a form of regulatory diplomacy, creating incentives for third countries to raise their data protection standards.

China's approach under the Personal Information Protection Law and the Data Security Law represents the opposite end of the spectrum. Localization is broadly mandated, cross-border transfers of important data and personal information require government security assessments, and the state retains expansive access to data held by private entities. China's model is explicitly sovereignty-centric, treating data as a strategic national resource.

The United States continues to lack a comprehensive federal data protection law, instead relying on a sectoral patchwork: The Health Insurance Portability and Accountability Act for medical data, the Gramm-Leach-Bliley Act for financial data, and the Children's Online Privacy Protection Act for data relating to children. This fragmented approach offers flexibility but creates compliance complexity for multinational entities and has come under increasing criticism in the context of transatlantic data flows.

India's hybrid model draws selectively from each of these approaches. Like the EU, it grounds data protection in constitutional rights and establishes a consent-based processing framework. Like China, it imposes strict localization requirements for financial data and reserves significant governmental powers. Like the United States, it adopts a sectoral approach that permits different rules for different types of data and different categories of entities. This eclecticism is both a strength—allowing India to calibrate its approach to domestic realities—and a potential weakness, as it generates normative tensions that require careful resolution.

9. Critical Assessment: Strengths and Unresolved Challenges

9.1 Achievements of the Current Framework

India's data protection framework represents a substantial advancement on the pre-2023 regulatory landscape. The DPDP Act provides a principled and coherent legal foundation for data protection, rooted in constitutional values and structured around the accountability of data fiduciaries. The establishment of the Data Protection Board creates, for the first time, a

dedicated institutional mechanism for enforcement and dispute resolution. The Act's extraterritorial application ensures that the protections it offers to Indian citizens are not circumvented by offshore processing. The RBI's localization regime, whatever its compliance costs, has demonstrably succeeded in ensuring that Indian payment data remains accessible to domestic regulatory and law enforcement authorities.

9.2 The Sensitive Data Classification Gap

The most significant structural criticism of the DPDP Act is its decision not to create a distinct category of sensitive personal data. Financial data—particularly when combined with location data, biometric identifiers, and behavioral analytics—can enable highly invasive profiling of individuals. The GDPR's special categories regime and the SPDI Rules' predecessor framework both recognized the heightened risks associated with certain categories of personal information. The DPDP Act's uniform treatment of all personal data, relying instead on the Significant Data Fiduciary designation to calibrate obligations, may not adequately address the particularized risks that financial data poses to individual privacy and dignity.

9.3 Government Exemptions and Accountability

The Act contains broad exemptions that allow the government to restrict the application of its provisions in the interests of national security, public order, and the sovereignty of India. Critics have argued that these exemptions, which are wider than comparable provisions in the GDPR, create a significant accountability deficit. If government agencies—including law enforcement and intelligence services—are substantially exempt from the Act's obligations, the Act's promise of informational privacy as a fundamental right is substantially diluted. The Puttaswamy judgment's proportionality requirement imposes some constitutional constraint on such exemptions, but the precise scope of permissible governmental exemptions remains contested.

9.4 Regulatory Uncertainty and the Absent Blacklist

The failure to publish a list of restricted countries under Section 16 has created a regulatory vacuum that undermines planning certainty for financial institutions. While the default-permissive model is commercially advantageous, the government's retention of an open-ended power to restrict transfers at any time, without clear criteria or advance notice, creates a climate of regulatory uncertainty. Financial institutions planning multi-year investments in data

infrastructure require predictable regulatory conditions; the current indeterminacy is antithetical to this need.

9.5 The Dual Compliance Burden

The coexistence of the DPDP Act and the RBI's regulatory framework creates a layered compliance burden that is particularly onerous for smaller financial institutions and fintech startups. Compliance with both frameworks requires legal expertise, technology investment, and operational coordination that larger entities can more readily absorb. There is a risk that the regulatory architecture disproportionately advantages incumbents over new entrants, potentially dampening the innovation that India's digital financial sector requires. Estimates suggest that compliance costs for financial institutions run to between five and ten percent of annual IT budgets, a non-trivial expenditure that should inform the design of any future regulatory reform.

9.6 Absent Rights in the Financial Context

The DPDP Act's omission of data portability rights and protections against automated decision-making is particularly significant in the financial context. Credit scoring, algorithmic lending, and fraud detection systems increasingly use automated analysis of personal financial data to make decisions with material consequences for individuals. The absence of a right to contest or seek explanation for such automated decisions leaves data principals without meaningful recourse. The introduction of rights comparable to Articles 21 and 22 of the GDPR would significantly enhance the Act's utility in the financial sector.

10. Conclusion

India's approach to the governance of cross-border financial data transfers reflects, in microcosm, the broader challenge facing all jurisdictions in the digital age: how to construct a regulatory framework that simultaneously protects individual rights, serves national security and economic interests, and remains compatible with the requirements of global commerce. The DPDP Act, 2023, and the RBI's sectoral regulations together constitute a hybrid architecture that draws on elements of the EU's rights-based model, China's sovereignty-centered approach, and the United States' sectoral pragmatism.

This architecture has achieved several important objectives. It has grounded data protection in constitutional values, established institutional enforcement mechanisms, imposed meaningful

accountability obligations on large data fiduciaries, and ensured that Indian payment data remains within the reach of domestic regulatory oversight. The case studies examined in this article demonstrate that even globally dominant platforms have been required to adapt their data practices to comply with India's localization requirements, lending credibility to the regulatory regime.

Nevertheless, significant work remains. The absence of a sensitive data category leaves financial data without the heightened protection its inherent risks demand. The non-publication of a restricted country list generates regulatory uncertainty that is inimical to long-term investment planning. Broad governmental exemptions create accountability deficits that sit uneasily with the Puttaswamy judgment's proportionality requirements. The absence of data portability and automated decision-making rights leaves individuals without adequate protection against algorithmic financial governance. And the cumulative compliance burden of navigating two overlapping regulatory frameworks risks creating structural barriers to entry in financial services.

Addressing these gaps requires legislative action—particularly the introduction of a sensitive data category and the clarification of cross-border transfer conditions—as well as regulatory coordination between the Data Protection Board and the Reserve Bank of India. A formal inter-regulatory coordination mechanism, perhaps modelled on the Financial Stability and Development Council that already coordinates financial regulation in India, could help align the two frameworks and reduce compliance complexity. International engagement through bilateral data sharing agreements and adequacy negotiations would also enhance the predictability and global compatibility of India's regulatory regime.

Ultimately, the measure of India's data protection framework will not be found in the sophistication of its statutory text but in the quality of its implementation: the independence of the Data Protection Board, the rigor of its enforcement, the responsiveness of regulators to evolving technological realities, and the genuine protection afforded to the hundreds of millions of Indian citizens whose financial data courses through digital systems every day. India has laid a credible foundation. The task now is to build upon it with the clarity, accountability, and institutional courage that the constitutional commitment to privacy demands.

References

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
3. Kharak Singh v. State of U.P., AIR 1963 SC 1295.
4. R.C. Cooper v. Union of India, (1970) 1 SCC 248.
5. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India).
6. Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
7. Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament (India).
8. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
9. Reserve Bank of India, Circular on Storage of Payment System Data, April 6, 2018.
10. Reserve Bank of India, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023.
11. Reserve Bank of India, Framework for Payment Aggregators – Cross-Border, 2023.
12. Payment and Settlement Systems Act, 2007, No. 51 of 2007, Acts of Parliament (India).
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Official Journal of the European Union, L 119.
14. Personal Information Protection Law of the People's Republic of China, 2021.
15. Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, 2018).
16. Arghya Sengupta, 'The Personal Data Protection Bill: An Analysis' (Vidhi Centre for Legal Policy, 2020).
17. Vrinda Bhandari and Renuka Sane, 'The Proposed Data Protection Framework in India: An Analysis of the India's Telecom Regulatory Authority of India Recommendations' (2019) 15 Indian Law Review 22.
18. Chinmayi Arun, 'On WhatsApp, Platforms, and Power' (2019) 8 Cambridge International Law Journal 164.
19. Graham Greenleaf, 'India's New Data Protection Law: A Critical Analysis' (2023) 9(4) International Data Privacy Law 267.
20. Reserve Bank of India, Report of the Internal Working Group on Digital Payments and Data Localization (2018).