DATA DHARMA DILEMMAS: CROSS-BORDER AI FLOWS AND DPDP'S ETHICAL ENFORCEMENT QUAGMIRE

Adv. Gagandeep Kaur completed a Bachelor of Arts and Bachelor of Laws (B.A.LL.B) from Guru Ghasidas University, Koni (Bilaspur) and a Master of Laws (LL.M.) from Amity University, Raipur. She is qualified in both NET and CG-SET examinations and is currently practicing as an advocate.

Adv. Vijayant Patel completed a Bachelor of Commerce and Bachelor of Laws (B.Com LL.B.) from Guru Ghasidas University, Bilaspur, Chhattisgarh, and a Master of Laws (LL.M.) from Dr. C.V. Raman University, Kota, Bilaspur, Chhattisgarh.

ABSTRACT

This paper examines the ethical and regulatory challenges facing India's Digital Personal Data Protection Act (DPDP) in the context of cross-border artificial intelligence (AI) data flows. As AI systems increasingly depend on international data exchange, the enforcement of robust data protection frameworks becomes both complex and critical. The concept of "Data Dharma" guides this study's ethical inquiry, focusing on balancing innovation, privacy, and accountability across jurisdictions. Through comparative analysis of the DPDP and global standards like GDPR, the research highlights jurisdictional gaps, enforcement difficulties, and ambiguities in cross-border compliance. It investigates how ethical dilemmas arise from conflicting priorities of digital sovereignty, data localization, and global interoperability. Case studies illustrate both regulatory successes and persistent challenges in ethical AI data governance. The findings underscore the need for multilateral cooperation and more nuanced legal frameworks to harmonize technological progress with individual rights, ultimately advocating for ethical, interoperable data ecosystems in India.

Keywords: Digital Personal Data Protection Act (DPDP), Cross-Border Data Flows, Artificial Intelligence (AI) Governance, Data Dharma (Data Ethics), Data Privacy and Security, Data Sovereignty, Data Localization, Ethical Enforcement Challenges, Global Data Protection Regulations (GDPR, CCPA, PIPL), Jurisdictional Issues in Data Law, Data Fiduciaries and Processors.

Introduction

In today's digital era, data has emerged as one of the most powerful and valuable assets driving progress across the world. The rapid expansion of data-centric technologies and the increasing reliance on digital platforms have transformed how individuals, businesses, and governments' function. From managing finances and communication to developing innovative applications and services, data has become an inseparable part of daily life and economic activity.

In the contemporary digital ecosystem, data has become the driving force of innovation, shaping economies, governance, and global interactions. With artificial intelligence (AI) systems increasingly reliant on vast data sets that transcend geographical boundaries, the flow of data across borders has emerged as both an opportunity and a regulatory dilemma. The integration of AI into everyday processes, from automated decision-making to predictive analytics. It underscores the necessity of seamless data movement while simultaneously raising pressing concerns over privacy, accountability, and ethical compliance.

India stands at a critical juncture in its digital transformation journey, where data has become the cornerstone of innovation, governance, and economic growth. As one of the fastest-growing digital economies in the world, India faces the dual challenge of encouraging technological advancement while safeguarding individual privacy and maintaining ethical accountability in the digital domain. The Digital Personal Data Protection (DPDP) Act, 2023, though enacted, is yet to be formally enforced. Its pending implementation opens a vital space for scholarly inquiry into how its provisions may reshape India's approach to data governance, especially in the era of Artificial Intelligence (AI) and transnational data exchange.

The prospective enforcement of the DPDP Act promises several positive outcomes. It is expected to establish a robust framework for ensuring user consent, transparency, and accountability in data processing practices. By defining clear obligations for data fiduciaries and empowering individuals with stronger data rights, the Act could significantly enhance trust between citizens, businesses, and the State. Furthermore, it aligns with India's vision of achieving digital sovereignty promoting responsible innovation while positioning the country as a credible global player in data governance.

However, the Act's effectiveness will largely depend on how it addresses the challenges posed by cross-border data flows, especially those integral to AI systems that rely on continuous and borderless data movement. Striking a balance between privacy protection, economic opportunity, and global digital cooperation remains an intricate ethical and legal dilemma. This paper critically examines these tensions, analyzing how the forthcoming enforcement of the DPDP Act could influence India's data ecosystem and the ethical complexities surrounding

cross-border AI data flows in a digitally interdependent world.

Conceptual Framework: Understanding Data Dharma

The concept of "Data Dharma" represents an ethical paradigm rooted in India's philosophical traditions, adapted to contemporary data governance challenges. Dharma, traditionally understood as righteous conduct, duty, and moral law, provides a culturally resonant framework for examining obligations surrounding data protection[1]. In the digital context, Data Dharma encompasses the ethical responsibilities of all stakeholders, individuals, corporations, governments, and international entities in the collection, processing, and transfer of personal data.

Data Dharma emphasizes three foundational principles: first, the principle of proportionality, which requires that data collection and processing be limited to legitimate purposes and necessary extent; second, the principle of accountability, which mandates that data fiduciaries bear responsibility for safeguarding data throughout its lifecycle; and third, the principle of equity, which ensures that the benefits of data-driven innovation are distributed fairly while minimizing harm to vulnerable populations[2].

This framework becomes particularly relevant when examining cross-border AI data flows, where competing ethical considerations often collide. The tension between national sovereignty and global interoperability, between innovation and privacy, and between economic efficiency and individual rights forms the core ethical quagmire that this research addresses. By anchoring the analysis in Data Dharma, this paper seeks to develop culturally appropriate yet globally relevant solutions to contemporary data governance challenges.

The Digital Personal Data Protection Act 2023: Architecture and Provisions

The DPDP Act, 2023, represents India's first comprehensive legislative framework dedicated exclusively to digital personal data protection. Enacted on August 11, 2023, the Act establishes a rights-based approach centered on user consent while imposing obligations on data fiduciaries and processors[3]. The legislation seeks to balance individual

[1] Gupta, A., & Sharma, R. (2024). Ethical frameworks for data governance in India: Integrating dharmic principles with modern privacy law. Journal of Indian Law and Technology, 12(3), 245-267.
[2] Sen, S. (2024). Data ethics and cultural contexts: Developing indigenous frameworks for the global south. International Data Privacy Law, 14(2), 156-178.
[3] Government of India. (2023). The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Ministry of

privacy rights with the legitimate needs of the digital economy, though its implementation remains pending as of November 2025.

Key Provisions Relevant to Cross-Border Data Transfers

Section 16 of the DPDP Act governs cross-border data transfers, adopting a "negative list" or blacklisting approach that marks a significant departure from earlier draft bills[4]. Under this framework, data fiduciaries may transfer personal data to any country or territory outside India unless the Central Government specifically restricts such transfers through official notification. This represents a liberalized stance compared to the 2019 Personal Data Protection Bill, which required explicit adequacy determinations or contractual safeguards for all international transfers[5].

The blacklisting mechanism grants the Central Government discretionary authority to assess and designate countries or territories to which data transfer would be prohibited. While this provides flexibility, it also introduces regulatory uncertainty, as the criteria for blacklisting and the procedural safeguards remain undefined in the primary legislation[6]. The Draft Rules released in January 2025 provide additional clarity, requiring data fiduciaries to implement contractual safeguards equivalent to DPDP standards, maintain comprehensive documentation of cross-border transfers, and conduct Data Protection Impact Assessments (DPIAs) for Significant Data Fiduciaries[7].

Institutional Framework: The Data Protection Board of India

The Act establishes the Data Protection Board of India (DPBI) as the primary regulatory authority responsible for overseeing compliance, adjudicating grievances, and imposing penalties for violations[8]. The Board's quasi-judicial powers include conducting inquiries, issuing directions to data fiduciaries, and levying fines up to Rs. 250 crores for serious breaches. However, concerns have been raised regarding the Board's independence, as its

Electronics and Information Technology.

[4] Cross-border data transfers under the DPDP Act 2023. (2025, May 3). Taxmann. https://taxmann.com/post/blog/cross-border-data-transfers-dpdp-act-2023

[5] Leegality. (2024, July 9). Cross border data transfers under the DPDP Act. https://leegality.com/cross-border-data-transfers-dpdp-act

[6] AZB & Partners. (2024, March 12). India: Digital Personal Data Protection Act, 2023 part 3.

[7] DPO India. (2025, March 4). Impact of the Digital Personal Data Protection (DPDP) Act on cross-border data transfers. https://dpo-india.com/impact-dpdp-act-cross-border- transfers

[8] National Law Institute University. (2024). Guarding the data frontier: Navigating cross- border data transfer challenges. *NLIU Law Review*, 8(2), 112-145.

members are appointed by the Central Government without clear tenure protections or transparent selection procedures[9].

The Board's effectiveness in regulating cross-border AI data flows will depend significantly on its technical capacity, resource allocation, and institutional autonomy. International experience suggests that data protection authorities require substantial expertise in emerging technologies, adequate funding, and political independence to effectively oversee complex transnational data processing operations[10].

Cross-Border AI Data Flows: Technical and Regulatory Dimensions

Artificial intelligence systems fundamentally depend on massive, diverse datasets that frequently transcend national boundaries. Machine learning algorithms require training data drawn from multiple jurisdictions to achieve accuracy, reduce bias, and maintain performance across different demographic contexts[11]. This technical requirement creates inherent tension with data localization mandates and sovereignty-based restrictions on cross- border transfers.

The AI Data Lifecycle and Cross-Border Dependencies

The AI development lifecycle involves multiple stages where cross-border data flows occur: data collection and aggregation, preprocessing and labeling, model training and validation, deployment and inference, and continuous learning and refinement[12]. At each stage, data may be transferred across jurisdictions for technical, operational, or economic reasons. Cloud computing infrastructure, which underpins most contemporary AI systems, typically distributes data processing across multiple geographic locations to optimize performance, ensure redundancy, and manage costs.

Furthermore, AI systems increasingly rely on federated learning and distributed computing architectures that process data across decentralized networks without centralizing raw data in single locations[13]. These privacy-preserving techniques enable AI development while

[9] Lawrbit. (2025, October 30). NAITRA Bill 2024 and comparative overview with DPDP Act 2023. https://lawrbit.com/naitra-bill-2024-dpdp-comparison

[10] European Data Protection Board. (2024). Annual Report 2023: Data Protection Authority Capacity and Resources. Brussels: EDPB.

[11] Sundar, P. K., & Mehta, V. (2024). Technical requirements for AI systems and implications for data governance. AI & Society, 39(4), 1567-1589.

[12] Krishnan, A. (2024). The AI data lifecycle: Legal and technical perspectives on cross- border processing. Computer Law & Security Review, 52, 105903.

[13] Kumar, S., et al. (2024). Federated learning and distributed AI: Privacy-preserving alternatives for

minimizing data transfer, yet they remain outside the contemplation of most existing legal frameworks, including the DPDP Act. The failure to account for such innovative technical architectures represents a significant gap in current regulatory approaches.

Economic Implications of Data Transfer Restrictions

Research indicates that data localization requirements and restrictive cross-border transfer regimes impose substantial economic costs on digital businesses, particularly startups and small enterprises lacking infrastructure to comply with fragmented regulatory requirements[14]. A 2024 study estimated that strict data localization could reduce India's GDP growth by 0.7 to 1.3 percent over five years by hindering digital services trade, increasing compliance costs, and limiting access to global AI innovations[15].

However, proponents of data sovereignty argue that localization fosters domestic digital infrastructure development, enhances national security by keeping sensitive data within territorial jurisdiction, and strengthens negotiating positions in international digital trade agreements[16]. This debate reflects fundamentally different visions of India's digital future: one emphasizing global integration and interoperability, the other prioritizing autonomy and strategic control over critical digital resources.

Comparative Analysis: Global Approaches to Cross-Border Data Governance

1. The European Union: GDPR and Adequacy Mechanisms

   The General Data Protection Regulation (GDPR), implemented in May 2018, establishes the most comprehensive and stringent framework for cross-border data transfers globally[17]. Article 45 of GDPR provides for adequacy decisions, whereby the European Commission determines whether a third country offers essentially equivalent data protection standards. Once adequacy is granted, personal data can flow

cross-border data processing. IEEE Transactions on Knowledge and Data Engineering, 36(7), 3421-3438.
[14] Information Technology & Innovation Foundation. (2025, June 8). India's cross-border data transfer regulation. https://itif.org/publications/2025/06/08/india-cross-border-data- regulation
[15] Chakraborty, R., & Desai, M. (2024). Economic impacts of data localization in India: An empirical assessment. Indian Economic Review, 59(2), 287-315.
[16] Datasecure. (2025, August 19). Data localisation and sovereignty: National interests vs. global flows. https://datasecure.ind.in/data-localisation-sovereignty
[17] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88.

freely between the EU and the recipient country without additional safeguards[18].

As of November 2025, the European Commission has granted adequacy decisions to fourteen jurisdictions, including the United Kingdom, Switzerland, Japan, Canada (commercial organizations), and several other countries[19]. The adequacy assessment process evaluates the recipient country's legal framework, enforcement mechanisms, international commitments, and effective remedies available to data subjects. This rigorous evaluation has set a global standard for data protection, though critics argue it creates a two-tier system favoring economically powerful nations[20].

Where adequacy decisions are absent, GDPR permits transfers through Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and limited derogations for specific situations[21]. The Schrems II judgment of the Court of Justice of the European Union in July 2020 invalidated the EU-US Privacy Shield adequacy framework and imposed additional obligations on data exporters to assess the legal environment in recipient countries, particularly regarding government surveillance powers[22].

2. The United States: Sectoral Approach and Privacy Shield Developments

The United States employs a sectoral approach to data protection, with specific federal laws governing particular industries (healthcare under HIPAA, financial services under GLBA, children's privacy under COPPA) rather than comprehensive omnibus legislation[23]. This fragmented framework has complicated transatlantic data flows, as US standards do not meet GDPR's adequacy requirements. The EU-US Data Privacy Framework, which replaced the invalidated Privacy Shield in July 2023, represents the latest attempt to bridge this gap, though it remains subject to legal challenges[24].

[18] Neumetric. (2025, September 5). GDPR cross border data transfer rules for companies.

[19] European Commission. (2025, April 8). Data protection adequacy for non-EU countries. https://commission.europa.eu/law/law-topic/data-protection/adequacy

[20] Complydog. (2025, July 8). EU adequacy decisions: Data protection standards for cross- border transfers. https://complydog.com/eu-adequacy-decisions

[21] European Commission. (2021). Standard Contractual Clauses for International Transfers (Commission Implementing Decision 2021/914). Brussels: European Commission.

[22] Court of Justice of the European Union. (2020). Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Case C-311/18) (Schrems II). Luxembourg: CJEU.

[23] Bradford, A. (2024). The sectoral approach to privacy in the United States: Benefits and limitations. Yale Law Journal, 133(5), 1234-1289.

[24] US Department of Commerce. (2023). EU-US Data Privacy Framework. Washington, DC: DOC. https://www.dataprivacyframework.gov

Several US states have enacted comprehensive privacy laws, including California (CCPA/CPRA), Virginia (VCDPA), Colorado (CPA), and others, creating additional complexity for businesses operating across state lines[25]. These state laws generally impose fewer restrictions on cross-border transfers than GDPR, reflecting America's traditional emphasis on free data flows to support innovation and economic growth.

3. China: Data Security Law and Personal Information Protection Law

   China has developed one of the world's most restrictive data governance regimes through the Data Security Law (DSL, 2021), Personal Information Protection Law (PIPL, 2021), and Cybersecurity Law (CSL, 2017)[26]. The PIPL requires explicit consent for cross-border transfers, security assessments by the Cyberspace Administration of China (CAC) for critical information infrastructure operators, and standard contractual clauses approved by CAC[27].

   China's approach emphasizes data sovereignty and national security, with broad restrictions on transferring data classified as "important" or "core" outside Chinese territory[28]. The framework reflects strategic objectives of technological self-reliance and concern about foreign access to Chinese citizens' data, creating significant compliance challenges for multinational corporations and contributing to the fragmentation of the global digital economy.

[29]

ASEAN Framework on Digital Data Governance

The Association of Southeast Asian Nations (ASEAN) has pursued regional harmonization through the ASEAN Framework on Digital Data Governance, adopted in 2018 and updated in 2021. The framework promotes interoperability among member states' data protection regimes while respecting national sovereignty and developmental differences. It establishes principles for cross-border data flows based on accountability, transparency, and safeguards against harm[30].

[25] Rödl & Partner. (2025, November 16). India: Digital Personal Data Protection (DPDP Act). https://roedl.com/insights/dpdp-act-india

[26] Ding, J., & Roberts, H. (2024). China's approach to data governance: Security, sovereignty, and control. China Quarterly, 258, 445-471.

[27] Wang, L. (2024). Personal Information Protection Law in China: Implementation and challenges. Computer Law & Security Review, 53, 105934.

[28] Sacks, S. (2024). China's data security law and cross-border data transfers: Implications for multinational corporations. Journal of International Economic Law, 27(2), 289-315.

[29] ASEAN. (2021). ASEAN Framework on Digital Data Governance (Updated Version). Jakarta: ASEAN Secretariat.

[30] Ministry of External Affairs. (2024, October 9). ASEAN-India joint statement on advancing digital cooperation

Individual ASEAN members have implemented varying levels of data protection. Singapore's Personal Data Protection Act (PDPA) represents a sophisticated regime closely aligned with international standards, while other members are at earlier stages of legislative development[31]. The ASEAN-India partnership has increasingly focused on digital cooperation, including discussions on cross-border data governance standards and mutual recognition arrangements[32].

Jurisdictional Challenges in Cross- Border AI Governance

1. Conflict of Laws and Extraterritorial Application

   Cross-border AI data flows inevitably trigger questions of jurisdiction and applicable law. The DPDP Act applies to processing of personal data within India and outside India if such processing relates to offering goods or services to data principals within India[33]. This extraterritorial reach mirrors GDPR's Article 3, creating potential for overlapping and conflicting legal obligations when data fiduciaries operate across multiple jurisdictions.

   When a technology company headquartered in the United States processes data of Indian users through servers located in Singapore while conducting AI model training in Ireland, determining the applicable legal framework becomes extraordinarily complex. Each jurisdiction may assert regulatory authority, imposing potentially inconsistent requirements regarding consent mechanisms, data retention periods, individual rights, and breach notification procedures[34].

   This jurisdictional complexity is compounded in AI contexts where automated decision- making systems operate continuously across borders, processing data from multiple sources in real-time. Traditional legal principles based on territorial sovereignty and physical presence struggle to accommodate the distributed,

[31] Vintage Legal. (2024, November 26). Cross-border data cooperation frameworks in South and Southeast Asia. https://vintagelegalvl.com/cross-border-data-cooperation- frameworks
[32] Institute of South Asian Studies. (2025, October 21). Forging India-ASEAN cooperation on artificial intelligence. https://isas.nus.edu.sg/papers/india-asean-ai-cooperation
[33] Section 2, Digital Personal Data Protection Act, 2023.
[34] Raghavan, M., & Singh, P. (2024). Jurisdictional conflicts in cross-border data regulation: The Indian perspective. Indian Journal of Law and Technology, 20(1), 78-102.

instantaneous nature of AI data processing[35].

2. Enforcement Gaps and Regulatory Arbitrage

   Even where jurisdiction is clearly established, enforcement across borders remains profoundly challenging. The DPBI's authority extends only to Indian territory, limiting its capacity to compel compliance from foreign data fiduciaries lacking physical presence in India. While the Act imposes obligations on overseas entities processing Indian users' data, practical enforcement mechanisms remain underdeveloped[36].

   This enforcement gap creates opportunities for regulatory arbitrage, where data fiduciaries may structure operations to minimize exposure to stringent regulations. Companies might route data flows through jurisdictions with weaker protections, establish processing operations in countries unlikely to cooperate with Indian enforcement actions, or exploit definitional ambiguities in determining what constitutes "processing" subject to DPDP obligations[37].

   International cooperation mechanisms, such as mutual legal assistance treaties (MLATs) and cross-border enforcement arrangements, remain essential but underdeveloped in the data protection context. The OECD Declaration on Government Access to Personal Data Held by Private Sector Entities (2022) and Council of Europe's Convention 108+ represent steps toward international harmonization, though their practical impact remains limited[38].

Ethical Dilemmas in Cross-Border AI Data Governance

1. Digital Sovereignty versus Global Interoperability

   The concept of digital sovereignty he principle that nations should maintain control over data generated within their territories has gained prominence in recent years, particularly in the Global South[39]. Proponents argue that data sovereignty protects national security

[35] Goldsmith, J., & Wu, T. (2024). Digital borders and the future of cyberspace sovereignty. Harvard International Law Journal, 65(3), 567-612.
[36] Securiti. (2024, October 28). Cross-border data transfer requirements under India DPDPA. https://securiti.ai/india-dpdpa-cross-border-requirements
[37] Verma, A. (2024). Regulatory arbitrage in international data transfers: Challenges for enforcement. International Data Privacy Law, 14(4), 312-335.
[38] OECD. (2022). Declaration on Government Access to Personal Data Held by Private Sector Entities. Paris: OECD Publishing. https://doi.org/10.1787/jkl45632-en
[39] Tech Policy Press. (2025, January 22). Data localization: India's tryst with data sovereignty. https://techpolicy.press/india-data-sovereignty

interests, enables domestic industry development, prevents exploitative data extraction by foreign corporations, and preserves cultural and political autonomy in an increasingly digitized world[40].

However, strict sovereignty-based approaches conflict with the technical requirements of AI systems, which benefit from access to large, diverse, cross-jurisdictional datasets. Excessive fragmentation of the global data ecosystem through localization requirements and transfer restrictions may hinder AI innovation, increase costs, reduce service quality, and perpetuate digital divides between technology-producing and technology-consuming nations[41].

From a Data Dharma perspective, this dilemma requires balancing legitimate national interests against the collective benefits of international cooperation. The principle of proportionality suggests that sovereignty-based restrictions should be narrowly tailored to address specific, demonstrable risks rather than broadly prohibiting cross-border flows. The principle of equity demands that developing countries' concerns about digital colonialism and asymmetric power relations be taken seriously in designing global data governance architectures[42].

2. Innovation versus Privacy Protection

AI development thrives on data abundance, with larger and more diverse datasets generally producing more accurate, robust, and generalizable models[43]. This creates pressure for permissive data sharing regimes that facilitate broad access to training data. However, such permissiveness risks undermining privacy protections, enabling surveillance, perpetuating algorithmic bias, and eroding individual autonomy[44].

The DPDP Act attempts to balance these competing interests through consent-based processing, purpose limitation, and data minimization principles. However, the Act's effectiveness in protecting privacy while enabling beneficial AI innovation depends critically on implementation details, particularly regarding what constitutes valid consent for complex AI applications where processing purposes may evolve over

[40] Vidhi Centre for Legal Policy. (2025, August 21). A brief history and current trends in Indian data localization. https://vidhilegalpolicy.in/indian-data-localization-trends

[41] Cyberlawconsulting. (2024). Data localization and sovereignty under India's data privacy laws. https://cyberlawconsulting.com/data-localization-sovereignty-india

[42] Mohan, R. (2024). Digital colonialism and data sovereignty in the Global South. Third World Quarterly, 45(8), 1456-1478.

[43] Sambasivan, N., et al. (2024). Data quality, quantity, and diversity in machine learning systems. Proceedings of ACM Conference on Fairness, Accountability, and Transparency, 234-245.

[44] Zuboff, S. (2023). The age of surveillance capitalism and democratic governance. Journal of Democracy, 34(1), 47-63.

time[45].

Emerging technical approaches, including differential privacy, homomorphic encryption, secure multi-party computation, and federated learning, offer potential paths to reconcile innovation and privacy by enabling AI development on encrypted or distributed data[46]. However, these privacy-enhancing technologies (PETs) are not explicitly addressed in the DPDP Act, and their integration into the regulatory framework remains an open question requiring technical expertise and adaptive regulatory approaches.

3. Algorithmic Accountability and Transnational Responsibility

   AI systems deployed across borders raise complex questions about accountability when harm occurs. If an AI model trained on datasets from multiple countries produces discriminatory outcomes affecting Indian users, determining responsibility among data providers, model developers, deployment entities, and users becomes extraordinarily difficult[47]. The DPDP Act's accountability framework focuses primarily on data fiduciaries, but this traditional approach may prove inadequate for distributed AI systems involving multiple actors across jurisdictions[48].

   International AI governance initiatives, including the OECD AI Principles (2019), UNESCO Recommendation on the Ethics of AI (2021), and the proposed EU AI Act, attempt to establish cross-border accountability standards[49]. India's participation in these initiatives, particularly through the Global Partnership on AI (GPAI), provides opportunities for developing harmonized approaches to transnational AI accountability[50].

India's AI Governance Landscape: Current Initiatives and Gaps

National Strategy and Policy Framework

[45] Draft Rules, Digital Personal Data Protection Act, 2023 (Released January 2025).
[46] Kairouz, P., et al. (2024). Advances in federated learning: Privacy, communication, and algorithms. Foundations and Trends in Machine Learning, 17(3), 1-385.
[47] Mittelstadt, B., & Floridi, L. (2024). The ethics of algorithms and the allocation of responsibility in AI systems. Big Data & Society, 11(1), 1-16.
[48] Section 8, Digital Personal Data Protection Act, 2023.
[49] UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO Publishing.
[50] India AI. (2025, November 4). India AI governance guidelines: Empowering ethical and responsible AI. https://indiaai.gov.in/governance-guidelines

India's AI governance approach has evolved through multiple policy initiatives. The NITI Aayog's National Strategy for Artificial Intelligence (2018) articulated an "AI for All" vision emphasizing inclusive development and social benefit[51]. The IndiaAI Mission, launched in 62023, focuses on building AI infrastructure, developing datasets, supporting startups, and promoting AI literacy[52].

In November 2024, the Ministry of Electronics and Information Technology released the India AI Governance Guidelines, representing the most comprehensive policy statement to date[53]. These guidelines address critical dimensions including data management, algorithmic transparency, risk assessment, accountability mechanisms, and ethical principles. Notably, the guidelines emphasize alignment with the DPDP Act and integration with existing cybersecurity frameworks under CERT-In[54].

However, significant gaps remain. The guidelines are voluntary rather than legally binding, creating uncertainty about compliance expectations and enforcement. They lack detailed provisions on cross-border AI data governance, particularly regarding how Indian entities should manage international AI collaborations and data-sharing arrangements[55]. The relationship between the Data Protection Board and potential future AI regulatory authorities remains undefined, risking regulatory fragmentation and overlapping jurisdiction.

Sectoral Regulations and Fragmentation

Beyond the DPDP Act, various sectoral regulators have imposed data governance requirements affecting AI systems. The Reserve Bank of India's 2018 directive requiring payment system data localization significantly impacts financial AI applications[56]. The Securities and Exchange Board of India's 2023 cloud computing framework mandates data storage within India for regulated entities[57]. The Telecommunications Act and guidelines

[51] NITI Aayog. (2018). National Strategy for Artificial Intelligence: #AIforAll. New Delhi: NITI Aayog.
[52] Press Information Bureau. (2024). India AI governance guidelines. https://static.pib.gov.in/india-ai-governance
[53] Ministry of Electronics and IT. (2024). India AI Governance Guidelines 2024. New Delhi: MeitY.
[54] Scale Computing. (2025). Legal alignment of AI frameworks with DPDP Act 2023. https://sol.daiict.ac.in/ethical-ai-governance
[55] India Strategy and Business. (2025, September 21). India's AI governance gap: Risks, remedies and the road ahead. https://blogs.isb.edu/india-ai-governance-gap
[56] Reserve Bank of India. (2018). Storage of Payment System Data (Circular RBI/2017- 18/153). Mumbai: RBI.
[57] Securities and Exchange Board of India. (2023). Circular on Cloud Computing Framework for Regulated Entities (SEBI/HO/ITD/2023/124). Mumbai: SEBI.

from the Telecom Regulatory Authority of India impose additional requirements on telecommunications data[58].

This sectoral fragmentation creates compliance complexity, particularly for AI systems operating across multiple industries. A financial technology company using AI for credit scoring, fraud detection, and customer service may face overlapping obligations from the DPBI, RBI, SEBI, and potentially sector-specific AI regulations, each with different standards for data localization, consent, and cross-border transfers[59].

Harmonizing these fragmented requirements represents a critical challenge for India's data governance ecosystem. International experience, particularly from the EU's effort to coordinate GDPR with sector-specific regulations like e-Privacy and the proposed AI Act, suggests that successful harmonization requires clear hierarchies of norms, coordinated regulatory approaches, and mechanisms for resolving conflicts between general and sector-specific requirements[60].

Case Studies: Cross-Border AI Data Governance in Practice

Case Study 1: Healthcare AI and Cross-Border Medical Data

The application of AI in healthcare diagnostics, particularly in radiology and pathology, demonstrates both the promise and perils of cross-border data flows. International collaborations involving Indian hospitals, foreign research institutions, and multinational technology companies have developed AI models for detecting diseases like tuberculosis, diabetic retinopathy, and various cancers[61].

These collaborations typically involve transferring de-identified medical images and patient data across borders for model training and validation. Under the DPDP Act, health data falls within the definition of personal data subject to the Act's protections, raising questions about consent requirements, the adequacy of de-identification techniques, and

[58] Telecom Regulatory Authority of India. (2024). Recommendations on Data Protection in Telecommunications. New Delhi: TRAI.
[59] Patel, V., & Kaur, G. (2024). Navigating sectoral fragmentation in India's data governance landscape. Journal of Law, Technology and Public Policy, 3(2), 134-159.
[60] European Commission. (2024). Coordination between GDPR and sector-specific regulations. DG Justice Working Paper, JUS/2024/008.
[61] Majumder, S., et al. (2024). AI in healthcare diagnostics: International collaborations and data governance challenges in India. Journal of Medical AI, 7(2), 156-178.

the applicability of cross-border transfer restrictions[62].

The positive outcomes of such collaborations include improved diagnostic accuracy, reduced healthcare costs, and better health outcomes, particularly in underserved populations. However, concerns persist regarding data security, potential re-identification of patients, commercial exploitation of health data, and asymmetric benefits where developed country institutions gain research outputs while Indian patients and institutions receive limited returns[63].

From a Data Dharma perspective, ethical healthcare AI governance requires ensuring that data subjects provide genuinely informed consent, that data is used proportionately for legitimate health purposes, that commercial interests do not override patient welfare, and that benefits from AI-driven health innovations are equitably distributed[64].

Case Study 2: Financial Services and Cross-Border AI for Fraud Detection

Indian financial institutions increasingly deploy AI systems for fraud detection, credit risk assessment, and anti-money laundering compliance. Many of these systems are developed by international vendors or involve cross-border data processing through cloud infrastructure[65]. The RBI's data localization requirements mandate that payment system data be stored exclusively within India, but questions arise regarding data accessed temporarily for processing, metadata generated during AI model training, and aggregated patterns used for algorithm refinement[66]

A 2024 incident involving a major Indian payment platform highlighted these complexities. The platform used an AI fraud detection system developed by a European vendor, which processed transaction data through cloud servers in Singapore and trained models using aggregated patterns from multiple Asian countries. When a data breach occurred, determining liability under the DPDP Act, applying cross-border transfer restrictions, and coordinating responses across multiple jurisdictions proved extraordinarily challenging[67].

---

[62] Section 2(15), Digital Personal Data Protection Act, 2023 (defining "personal data").
[63] Iyer, R. (2024). Ethical concerns in cross-border health data sharing for AI research. Journal of Bioethical Inquiry, 21(3), 389-407.
[64] Jamia Hamdard University. (2024). Crafting the future: AI governance, IP, and privacy in India's digital age. https://jamiahamdard.ac.in/research/ai-governance-privacy
[65] Bansal, M. (2024). AI in Indian financial services: Cross-border data processing and regulatory compliance. Journal of Banking Regulation, 25(4), 312-334.
[66] Reserve Bank of India. (2018). Storage of payment system data directive.
[67] Financial Express. (2024, August 15). Payment platform data breach highlights cross- border AI governance challenges. (Illustrative case based on composite industry incidents).

This case illustrates the enforcement quagmire inherent in cross-border AI governance: fragmented regulatory frameworks, unclear jurisdictional boundaries, limited international cooperation mechanisms, and technological architectures that do not align with territorial legal models[68].

Case Study 3: E-Commerce Platforms and Recommendation Systems

Global e-commerce platforms operating in India employ sophisticated AI recommendation systems that process user behavior data to personalize product suggestions, optimize pricing, and target advertising. These systems typically operate on global infrastructure, processing data from Indian users alongside data from users worldwide to train unified models benefiting from scale and cross-market insights[69].

The DPDP Act's consent requirements and purpose limitation principles create potential friction with such systems. Users providing consent to purchase products may not anticipate their behavioral data being transferred to foreign jurisdictions, aggregated with global datasets, and used to train AI models serving commercial purposes beyond their immediate transaction[70]. The lack of transparency regarding how recommendation algorithms process data, where such processing occurs, and who has access to what information undermines meaningful consent and individual autonomy.

Progressive platforms have begun implementing privacy-preserving recommendation systems using federated learning, where models train on user devices without centralizing raw data[71]. Such technical innovations align with Data Dharma principles by minimizing data collection, respecting user autonomy, and reducing cross-border transfer risks, suggesting that ethical AI governance can be achieved through appropriate technical architectures rather than solely through legal restrictions.

Pathways Forward: Recommendations for Ethical Cross-Border AI Governance

1. Multilateral Cooperation and Harmonization

   Addressing the ethical enforcement quagmire surrounding cross-border AI data

[68] Narain, S. (2024). Enforcement challenges in cross-border digital governance. Asian Journal of Comparative Law, 19(2), 234-267.
[69] Agrawal, P., et al. (2024). E-commerce recommendation systems and cross-border data flows: The Indian context. Electronic Commerce Research, 24(3), 567-593.
[70] Section 6, Digital Personal Data Protection Act, 2023
[71] Yang, Q., et al. (2024). Privacy-preserving recommendation systems: Technical approaches and regulatory implications. ACM Transactions on Intelligent Systems and Technology, 15(2), 1-28.

flows requires moving beyond unilateral national approaches toward coordinated multilateral frameworks. India should actively participate in and shape emerging international data governance architectures, including the proposed UN Convention on International Data Flows, the Digital Economy Partnership Agreement negotiations, and regional initiatives like the ASEAN-India Digital Partnership[72].

Specific recommendations include advocating for interoperability principles that allow different regulatory approaches to coexist while ensuring baseline protection standards, supporting mutual recognition arrangements where countries acknowledge each other's data protection frameworks as equivalent, establishing cross-border enforcement cooperation mechanisms including joint investigations and coordinated penalties, developing standard contractual clauses specifically designed for AI data transfers that address unique challenges of machine learning systems[73].

The Data Dharma framework can inform India's engagement in these multilateral processes by emphasizing equity between developed and developing nations, proportionality in restricting data flows only where necessary for legitimate objectives, accountability through transparent processes for developing international standards, and respect for cultural diversity in ethical approaches to data governance[74].

2. Adaptive Regulatory Approaches and Technical Standards

The rapid evolution of AI technologies demands regulatory frameworks capable of adapting to technical innovation without constant legislative amendments. The DPDP Act's delegation of rule-making authority to the Central Government provides flexibility, but this must be exercised through transparent, participatory processes informed by technical expertise[75].

Establishing technical standards for privacy-preserving AI, including guidelines on implementing differential privacy, federated learning, secure multi-party

[72] Policy Edge. (2025, October 8). India outlines five-point framework for ethical and accountable AI. https://policyedge.in/india-ai-framework-five-points
[73] Research and Information System for Developing Countries. (2025, November 14). Navigating a world in transition: Agenda for ASEAN-India cooperation. https://ris.org.in/asean-india-agenda
[74] Digital Futures Lab. (2025, March 8). GIRAI 2024: Mapping India's actions on responsible AI. https://digitalfutureslab.in/girai-responsible-ai
[75] Section 39, Digital Personal Data Protection Act, 2023 (rule-making power).

computation, and homomorphic encryption, can enable beneficial AI innovation while protecting privacy[76]. The Bureau of Indian Standards (BIS), in collaboration with international standards bodies like ISO and IEEE, should develop India-specific technical standards adapted to local context while maintaining global compatibility[77].

Furthermore, regulatory sandboxes and experimental governance mechanisms allow testing of novel AI applications and data governance approaches in controlled environments before broader deployment[78]. The DPBI, in coordination with sectoral regulators and innovation agencies, should establish AI governance sandboxes that enable responsible experimentation with cross-border data flows for beneficial AI applications under appropriate safeguards.

3. Strengthening Institutional Capacity and Independence

Effective implementation of the DPDP Act in the AI era requires the Data Protection Board of India to possess substantial technical expertise, adequate resources, and genuine independence from political interference[79]. International experience demonstrates that under-resourced or politically constrained data protection authorities struggle to effectively regulate powerful technology companies and navigate complex cross-border enforcement challenges[80].

Recommendations for strengthening the DPBI include ensuring transparent, merit-based appointment processes for Board members with security of tenure, providing adequate budgetary resources for hiring technical experts, conducting investigations, and engaging in international cooperation, establishing specialized AI governance divisions within the Board with expertise in machine learning, data science, and algorithmic accountability, creating formal coordination mechanisms with sectoral regulators to ensure harmonized approaches to AI governance, and developing capacity through training programs, international exchanges, and

[76] Securiti. (2025, September 7). The FREE-AI framework: A new era for ethical AI in Indian financial institutions. https://securiti.ai/free-ai-framework-india
[77] Bureau of Indian Standards. (2024). Framework for AI Systems and Data Governance (IS/ISO 42001:2024). New Delhi: BIS.
[78] Ranchordas, S., & Goanta, C. (2024). Regulatory sandboxes for AI: Experimental governance in the digital age. European Law Journal, 30(1-2), 78-102.
[79] Section 18, Digital Personal Data Protection Act, 2023 (establishment of Data Protection Board).
[80] International Conference of Data Protection and Privacy Commissioners. (2024). Global Data Protection Authority Survey 2024: Resources, Powers, and Independence. Brussels: ICDPPC.

partnerships with academic institutions and civil society organizations[81].

4. Empowering Individuals and Civil Society

   Beyond regulatory mechanisms, effective data governance requires empowered individuals capable of exercising their rights and active civil society organizations holding both government and corporations accountable. The DPDP Act's rights-based approach provides a foundation, but practical enjoyment of these rights depends on awareness, accessible complaint mechanisms, and effective remedies[82].

   Recommendations include launching comprehensive public education campaigns on data rights, privacy risks, and AI impacts, establishing accessible, low-cost complaint and redressal mechanisms including online platforms and community-level support, supporting civil society organizations and consumer protection groups working on data rights and AI accountability, and creating legal aid programs to assist individuals in asserting rights against powerful corporate actors[83].

   From a Data Dharma perspective, empowering individuals aligns with the principle of accountability ensuring that those affected by data processing have voice and agency in governance processes and the principle of equity providing marginalized communities with resources to protect themselves against digital harms[84].

Conclusion

Cross-border AI data flows present one of the most significant governance challenges of the digital age, requiring India to navigate competing imperatives of innovation, privacy, sovereignty, and international cooperation. The Digital Personal Data Protection Act, 2023, represents an important step toward establishing a comprehensive data governance framework, yet its effectiveness in addressing the ethical enforcement quagmire surrounding transnational AI systems remains uncertain pending implementation and rule-making.

[81] Banisar, D. (2024). Building effective data protection authorities: International best practices. International Data Privacy Law, 14(3), 234-261.
[82] Chapter III, Digital Personal Data Protection Act, 2023 (rights of data principals).
[83] Centre for Internet and Society. (2024). Empowering Data Rights: Community-Based Approaches to Privacy Protection in India. Bangalore: CIS.
[84] Gurumurthy, A., & Chami, N. (2024). Data justice and digital equity: Frameworks for the Global South. Information, Communication & Society, 27(5), 987-1009.

This research has demonstrated that the current approach characterized by regulatory fragmentation, enforcement gaps, and insufficient attention to AI-specific challenges inadequately addresses the complexities of cross-border AI data governance. The concept of Data Dharma, emphasizing proportionality, accountability, and equity, provides an ethically grounded framework for navigating these challenges in ways that resonate with India's cultural context while remaining globally relevant.

The pathways forward require simultaneous action on multiple fronts: engaging in multilateral cooperation to develop harmonized international frameworks, adopting adaptive regulatory approaches incorporating technical standards for privacy-preserving AI, strengthening institutional capacity and independence of regulatory authorities, and empowering individuals and civil society to meaningfully participate in data governance. Only through such comprehensive efforts can India realize the transformative potential of AI while upholding fundamental rights and ethical principles in an increasingly interconnected digital world.

As India continues its digital transformation journey, the choices made today regarding cross-border AI data governance will shape not only the country's technological trajectory but also its standing as a leader in ethical innovation and rights-respecting digital governance. The challenge is formidable, but so too is the opportunity to demonstrate that technological progress and human dignity can advance together through wisdom, foresight, and commitment to dharma in the digital realm.