FROM STATUTE TO NOTIFICATION: EXECUTIVE DISCRETION AND THE UNFINISHED ARCHITECTURE OF INDIA'S CROSS-BORDER DATA TRANSFER REGIME

Saveri Sourabh Sharma, NMIMS Kirit P. Mehta School of Law, Mumbai (2021-2026)

ABSTRACT

The Digital Personal Data Protection Act, 2023 replaced a decade of tiered, mirror-and-localise proposals with a single negative-list rule: personal data may leave India freely unless the Central Government names a destination as restricted. Read on its own, Section 16 looks like liberalisation. Read against the sectoral rules that survive it and against the discretion it hands the executive to define the negative list on unspecified terms, it looks narrower: a transfer of localisation power away from Parliament and into notification-making authority that Parliament barely constrains. This article asks whether the DPDP Act has produced a coherent cross-border transfer regime or has moved localisation decisions from legislative drafting to executive discretion. It traces the regulatory history that produced Section 16, places India's negative-list model within the comparative taxonomy of localisation instruments, and examines how the Reserve Bank of India, the Securities and Exchange Board of India, the Insurance Regulatory and Development Authority of India, and the telecommunications framework continue to impose transfer restrictions whether or not the Central Government ever exercises its Section 16 power. It also considers the Draft Digital Personal Data Protection Rules, 2025, whose Rule 12(4) reintroduces category-based localisation for Significant Data Fiduciaries that the Act's headline architecture appeared to have retired. The article argues that legal certainty, not the choice between openness and restriction, is the DPDP Act's principal deficit, and it proposes statutory criteria for the Section 16 power, coordination of the sectoral stack, and a more active Indian posture in multilateral data governance negotiations.

Keywords: data localisation, cross-border data transfer, digital sovereignty, DPDP Act 2023, executive discretion, data protection law, India

I. INTRODUCTION

Section 16 of the Digital Personal Data Protection Act, 2023 runs to a single operative sentence: the Central Government may, by notification, restrict the transfer of personal data to such countries or territories as it specifies.[1] Everything the statute has to say about cross-border data transfer sits in that sentence and the savings clause that follows it. There is no adequacy test, no list of factors the government must weigh, no procedure for a data fiduciary or a foreign government to contest a designation, and no sunset or periodic review requirement beyond the general practice of tabling notifications before Parliament.[2] Compared to the tiered, three-category localisation scheme the Srikrishna Committee proposed in 2018, or the mirroring and whitelisting variants that appeared in the Bills that followed it, Section 16 is strikingly spare.[3]

That sparseness has generally been read as liberalisation. The Office of the United States Trade Representative's 2024 National Trade Estimate Report described the shift from the 2019 Bill's restrictive posture to the DPDP Act's default-permissive rule as a positive development for market access, and industry commentary has largely agreed.[4] This article takes a different view of what the change actually accomplishes. A negative list that names no criteria for what belongs on it is not a rule; it is an unallocated power. Whether that power turns out to be liberal or restrictive in practice depends entirely on how, and how often, the executive chooses to use it, and on how much room the sectoral regulatory apparatus, the Reserve Bank of India's payments directive, SEBI's cloud circular, IRDAI's insurance guidelines, and the telecommunications trusted-source framework, leaves for Section 16 to matter at all.

The central claim developed here is that the DPDP Act has not resolved the question that occupied Indian data protection policy from 2017 onward, namely how much cross-border data flow the state is prepared to tolerate, and on what terms. It has instead relocated that question from the legislative process, where the Srikrishna Committee's tiered categories were at least debated and defended on the record, to executive notification-making, where no comparable scrutiny attaches. The Draft Digital Personal Data Protection Rules, 2025, released roughly

[1] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 16 (India) [hereinafter DPDP Act].
[2] Smriti Parsheera, *Data Protection and Cross-Border Data Flows in India*, Brussels Privacy Hub Working Paper, Vol. 10, No. 5, at 17 (Mar. 2024) [hereinafter Parsheera, *Cross-Border Data Flows*].
[3] Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Ministry of Elecs. & Info. Tech. (July 27, 2018) [hereinafter Srikrishna Comm. Report].
[4] Office of the U.S. Trade Representative, *2024 National Trade Estimate Report on Foreign Trade Barriers* 189–92 (USTR, 2024).

eighteen months after the parent Act, illustrates the point directly: Rule 12(4) permits the government to designate categories of personal data that Significant Data Fiduciaries may not transfer outside India at all, a form of localisation that operates independently of and in addition to Section 16's own negative list, introduced by delegated rule-making rather than by the amendment process that would ordinarily govern a change of this consequence.[5]

The argument proceeds in five parts. Part II situates the debate within the existing literature on data localisation and digital sovereignty, distinguishing analysis that treats India's posture as strategic ambiguity from analysis that treats it as regulatory drift. Part III sets out a conceptual framework, adopting the fourfold taxonomy of localisation instruments developed by Basu, Hickok, and Chawla and situating the DPDP Act's negative-list model within it. Part IV traces the statute's regulatory lineage and examines how the sectoral stack, RBI, SEBI, IRDAI, and telecommunications regulation, continues to impose transfer restrictions independently of Section 16. Part V offers a critical discussion of the costs this arrangement generates: for legal certainty, for the credibility of any future adequacy negotiation with the European Union, and for the compliance burden borne disproportionately by smaller Indian firms relative to large multinationals. Part VI sets out recommendations, and Part VII concludes.

II. LITERATURE REVIEW

The comparative literature on data localisation converges on a basic point of vocabulary before it diverges on normative assessment. Chander and Le's influential account frames localisation requirements as a species of "data nationalism," a protectionist instinct dressed in the language of privacy and security, and argues that most such requirements fail to achieve their stated security objectives while imposing real costs on digital trade.[6] Basu, Hickok, and Chawla take a more classificatory approach, mapping the spectrum from hard, exclusive localisation of the kind China's Cybersecurity Law and Russia's Federal Law No. 242-FZ impose, through mirroring requirements, to conditional transfer regimes and, at the most permissive end, negative-list systems.[7] Their 2019 study anticipated that India would eventually land on a

[5] Khushi Malviya & Eeshaan Singh, *Cross-Border Data Transfers and Data Localization Mandate under the Data Protection Regime* (discussing Rule 12(4) of the Digital Personal Data Protection Rules, 2025 (Draft)) [hereinafter Malviya & Singh].
[6] Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 Emory L.J. 677, 678 (2015).
[7] Arindrajit Basu, Elonnai Hickok & Aditya Singh Chawla, *The Localisation Gambit: Unpacking Policy Approaches to Cross-Border Data Flows* 8–14 (Ctr. for Internet & Soc'y, 2019) [hereinafter Basu, Hickok & Chawla].

negative-list model, reading it correctly as the outcome most compatible with a state that wants to preserve room to restrict without committing to a restrictive baseline.[8]

A second strand of the literature treats India's posture less as a considered policy choice and more as the product of institutional layering. Parsheera's early work on the RBI's payments directive found that the central bank's stated supervisory objectives could have been achieved through contractual access clauses and mutual legal assistance mechanisms considerably less restrictive than outright domestic storage, and her 2024 study extends that critique to the DPDP Act itself, observing that the Act's liberal transfer default coexists with, and does nothing to discipline, a proliferating set of sector-specific restrictions in payments, telecommunications, and public records.[9] That second study is particularly useful here because it documents, with more currency than the Act's own legislative history permits, how India has approached cross-border data questions in its trade diplomacy: the country's continued absence from the WTO's Joint Statement Initiative on E-commerce, its light-touch electronic-flow language in the UAE and Singapore economic agreements, its more substantive financial-data transfer commitment to Japan, and its ongoing resistance to binding digital-trade provisions in the negotiations with the United Kingdom.[10]

A third body of work approaches the question through the lens of digital sovereignty rather than trade law. Reddy situates India's localisation instincts within the "data colonialism" critique, the view that unrestricted data flows from the Global South disproportionately enrich platforms headquartered in the Global North, while noting that Indian policy discussions have not clearly shown how local storage requirements would actually increase domestic access to, or innovation from, that data.[11] Kaya and Shahid's comparative review of digital sovereignty as a legal concept makes a related observation at a more general level: sovereignty claims over data are increasingly used to justify a wide range of regulatory interventions whose relationship to any coherent theory of sovereignty is often asserted rather than demonstrated.[12] Gupta's survey of India's localisation measures reaches a similar conclusion from a domestic

[8] Basu, Hickok & Chawla, supra note 8.
[9] Smriti Parsheera, *Data Localisation in India: Questioning the Means and Ends*, Nat'l Inst. of Pub. Fin. & Pol'y, Working Paper No. 228, at 4–9, 12–16 (2018) [hereinafter Parsheera, *Questioning the Means and Ends*]; Parsheera, *Cross-Border Data Flows*, supra note 3, at 17–19.
[10] Parsheera, *Cross-Border Data Flows*, supra note 3, at 17–19.
[11] Shashank Reddy, *India's Approach to Cross-Border Data Flows*, Alternative Futures, Goethe-Institut/Max Mueller Bhavan (Dec. 2023).
[12] Mehmet Kaya & Hamza Shahid, *Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance*, 4(2) Interdisc. Stud. in Soc'y, L. & Pol. 219, 219–33 (2025).

administrative-law angle, arguing that the multiplicity of sectoral instruments, RBI, SEBI, IRDAI, and now the DPDP framework, has produced a patchwork whose cumulative effect is considerably more restrictive than any single instrument suggests on its own.[13]

A fourth and more recent strand examines the Draft DPDP Rules, 2025 directly. Malviya and Singh's analysis of Rule 12(4) and Rule 14 argues that the Draft Rules walk back the liberal posture the Act itself signalled, introducing a form of category-based localisation for Significant Data Fiduciaries that operates without any published criteria for how the underlying data categories or fiduciary designations will be made, and without addressing the "onward transfer" gap that leaves data unregulated once it reaches a permitted destination.[14] Their comparison with the GDPR's more structured mechanism, adequacy findings, standard contractual clauses, binding corporate rules, is instructive precisely because it shows what a negative-list system could look like if it specified criteria, and what India's currently does not.

What is missing from this literature, and what this article tries to supply, is a sustained account of how these four strands connect: how the negative-list model's formal openness interacts with the sectoral stack's persistent restrictiveness, and how the 2025 Draft Rules confirm, rather than answer, the concern that the DPDP Act shifted rather than resolved the localisation question.

III. CONCEPTUAL FRAMEWORK

A. *A Taxonomy of Localisation Instruments*

Basu, Hickok, and Chawla's fourfold taxonomy remains the most analytically useful frame for placing the DPDP Act's transfer regime.[15] At the most restrictive end sits hard or exclusive localisation, under which data may be stored and processed only on domestic infrastructure; China's Cybersecurity Law and Russia's data localisation statute approximate this model.[16] One register down is mirroring localisation, which permits international transfer but requires that a domestic copy also be retained, the approach the Srikrishna Committee proposed for

[13] Vivek Kumar Gupta, *Data Localization and Digital Sovereignty in India: Navigating the Crossroads of Privacy, Security, and Global Trade*, 7(8) Int'l J. of Multidisciplinary Trends 36, 36–45 (2025).
[14] Malviya & Singh, supra note 6.
[15] Basu, Hickok & Chawla, supra note 8.
[16] *Id.*; China Cybersecurity Law (promulgated by the Standing Committee of the National People's Congress, Nov. 7, 2016, effective June 1, 2017) (P.R.C.).

"sensitive personal data" in 2018.[17] Less restrictive still is conditional localisation, which allows cross-border transfer subject to an adequacy finding, standard contractual clauses, or comparable safeguards, the model the GDPR's Chapter V embodies.[18] At the most permissive end sits the negative-list approach: transfers are freely allowed unless government has affirmatively designated a destination as restricted.

Formally, Section 16 belongs at this permissive end. But the taxonomy's ordering assumes that each category carries a reasonably predictable degree of restrictiveness in practice, and that assumption breaks down for a negative list that specifies no criteria for its own operation. A conditional-transfer regime with a defined adequacy standard, of the kind the GDPR applies, is more restrictive on its face than a negative list, yet it is also more predictable: a data fiduciary can assess, in advance, whether a given transfer will pass muster. A negative list without criteria offers the opposite trade: less restriction most of the time, but no way to know in advance whether or when that will change. Sen and Chadha's 2024 comparative study of negative-list systems among large developing economies makes a related point, describing the model as a device for preserving regulatory flexibility while projecting openness to digital trade, a description that fits India's posture closely but that this article situates more specifically within the constitutional and institutional constraints unique to it.[19]

B. *Digital Sovereignty as an Organising Idea*

Digital sovereignty gained real purchase in policy discourse after 2013, when disclosures about the scale of United States signals-intelligence collection prompted a broad reassessment of dependence on infrastructure controlled by a small number of jurisdictions.[20] At its simplest the concept asserts a state's claim to exercise meaningful authority over digital activity within its territory and over its nationals. UNCTAD's 2021 Digital Economy Report frames that claim in developmental terms: the case for sovereignty strengthens considerably where data generated by one country's population is systematically monetised by firms headquartered elsewhere, producing a concentration of digital value that development economists

[17] Srikrishna Comm. Report, supra note 4.
[18] Council Regulation 2016/679, 2016 O.J. (L 119) 1 (General Data Protection Regulation), arts. 44–49 [hereinafter GDPR].
[19] Basu, Hickok & Chawla, supra note 8 (citing the negative-list model's function of preserving regulatory flexibility while projecting openness to digital trade).
[20] U.N. Conf. on Trade & Dev., *Digital Economy Report 2021: Cross-Border Data Flows and Development* 8–14 (2021) [hereinafter UNCTAD].

increasingly treat as a structural feature of the contemporary data economy rather than an incidental byproduct of it.[21]

India's own account of its data governance choices draws heavily on this framing, but Kaya and Shahid's broader review of digital sovereignty as a governance concept is a useful corrective here: sovereignty rhetoric is capacious enough to justify almost any regulatory intervention, from genuine security-driven storage requirements to measures whose real function is industrial policy dressed in sovereignty language.[22] The DPDP Act's negative-list structure is built to preserve the executive's capacity to invoke either justification as needed, restricting a destination for a documented security reason, or for reasons closer to digital protectionism, without the statute requiring it to say which is operating in a given case.

C. *Cross-Border Flows and Economic Stakes*

The economic case against restrictive localisation is well established empirically, even if its policy implications remain contested. The McKinsey Global Institute's often-cited 2016 estimate found that cross-border data flows had already come to contribute more to global GDP growth than traditional trade in goods.[23] For India specifically, the IT and business-process outsourcing sectors generate roughly $245 billion in annual revenue and employ more than 5.4 million people directly, an industry whose competitive position rests substantially on the ability to process data collected abroad on Indian infrastructure.[24] The OECD has documented that localisation requirements raise data-management compliance costs by 30 to 60 per cent, a burden that falls disproportionately on smaller firms with less capacity to absorb duplicate infrastructure spending.[25] The Indian Council for Research on International Economic Relations has estimated that a one per cent reduction in cross-border data flows could cost India approximately $696.71 million in trade.[26]

None of this settles the normative question. UNCTAD's distributional critique is a serious one: unconditional data-flow liberalisation does carry different consequences for economies whose digital industries are not yet globally competitive than for economies whose firms already

[21] UNCTAD, supra note 21.
[22] Kaya & Shahid, supra note 13, at 224–28.
[23] McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows* (2016).
[24] NASSCOM, *India IT-BPM Sector Annual Report 2024* (NASSCOM, 2024).
[25] OECD, *Digital Trade and Data Flows: A Framework for Analysis* (2019).
[26] Reddy, supra note 12.

operate at global scale, and that asymmetry is the analytical foundation for India's developmental-state posture on data governance.[27] The point this article makes is narrower. Whatever position India takes on that underlying trade-off, restriction or openness, the position needs to be legible in advance to the firms and foreign counterparts who have to plan around it. A negative list without criteria delivers neither predictable openness nor a defensible restriction; it delivers discretion, and discretion is not, by itself, a governance outcome.

IV. ANALYSIS

A. *The Road to Section 16*

For roughly two decades after the liberalisation of India's telecommunications sector, cross-border data flows were largely absent from the domestic policy agenda. The Information Technology Act, 2000, modelled on the UNCITRAL Model Law on Electronic Commerce, addressed electronic authentication, digital signatures, and cybercrime, not data protection as such, and the transfer-related provisions later inserted through Section 43A and the 2011 Sensitive Personal Data Rules were so heavily qualified by consent requirements that they imposed no meaningful restriction in practice.[28] Parsheera's account of this period is apt: the openness was not a deliberate policy choice so much as regulatory inattention to the privacy and security implications of large-scale outsourced data processing, an inattention that suited an IT sector whose commercial model depended on it.[29]

The first real departure came not from Parliament but from a central bank circular. On 6 April 2018 the Reserve Bank of India issued its Master Direction on Storage of Payment System Data, requiring all payment-system operators to store payment-related data exclusively on systems located in India and to delete any data previously held abroad after migration.[30] The directive drew sustained opposition from international payment networks and was flagged as a trade barrier in the USTR's 2019 National Trade Estimate Report.[31] The RBI held its position; by 2021 it had suspended new-customer onboarding for foreign payment operators that had not

[27] UNCTAD, supra note 21.
[28] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 7.
[29] Parsheera, *Questioning the Means and Ends*, supra note 10, at 4–9.
[30] Reserve Bank of India, Master Direction on Storage of Payment System Data, DPSS.CO.OD No. 2785/06.08.005/2017-18 (Apr. 6, 2018) [hereinafter RBI Master Direction]; Payment and Settlement Systems Act, 2007, § 10(2), No. 51, Acts of Parliament, 2007 (India).
[31] Office of the U.S. Trade Representative, *2019 National Trade Estimate Report on Foreign Trade Barriers* (USTR, 2019).

complied. Parsheera's analysis shows that the RBI's stated supervisory objectives, access for regulatory oversight, consumer protection, and national security, could have been achieved through less restrictive alternatives, mandatory contractual access clauses or mutual legal assistance frameworks among them, which makes the 2018 directive the clearest instance in India's regulatory landscape of what Chander and Le would classify as data nationalism rather than narrowly tailored regulation.[32] The directive has never been tested on constitutional grounds directly; the Supreme Court's decision in the related cryptocurrency circular case, which applied a proportionality standard to a different RBI measure, leaves the payments directive's own proportionality formally unresolved.[33]

The Justice B.N. Srikrishna Committee, reporting in July 2018, proposed a considered alternative: a three-tier framework distinguishing critical personal data subject to exclusive domestic storage, sensitive personal data permitted to move internationally subject to a mandatory domestic mirror copy, and all other personal data left to flow freely subject to standard contractual safeguards.[34] The Committee explicitly considered and rejected hard localisation across all categories, finding that supervisory access and privacy protection could both be secured through a conditional-transfer framework paired with robust consent and accountability requirements, a finding that matters because it amounts to an official acknowledgement, on the record, that less restrictive alternatives to comprehensive localisation were available and had been weighed.[35]

The Personal Data Protection Bill, 2019 largely carried the Committee's tiered structure forward.[36] The Joint Parliamentary Committee's report of December 2021 recommended expanding the sensitive-data category and broadening government exemptions, changes the Internet Freedom Foundation and other civil-society and academic commentators criticised as building a surveillance architecture at odds with the proportionality framework the Supreme Court's privacy jurisprudence requires.[37] The Union Government withdrew the Bill in August 2022, a move widely understood as reflecting both this domestic pressure and external pressure

[32] Parsheera, *Questioning the Means and Ends*, supra note 10, at 12–16; Chander & Le, supra note 7.
[33] Internet and Mobile Association of India v. Reserve Bank of India, W.P. (Civil) No. 528 of 2018 (Mar. 4, 2020) (India).
[34] Srikrishna Comm. Report, supra note 4.
[35] *Id.*
[36] Personal Data Protection Bill, 2019, Bill No. 373 of 2019, Gazette of India (Dec. 11, 2019).
[37] Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, Report of the Joint Committee of Parliament (Dec. 16, 2021); Internet Freedom Foundation, *Analysis of the Digital Personal Data Protection Act, 2023* (2023).

from the United States government and technology industry to soften the localisation provisions. The 2022 draft that briefly followed proposed a whitelisting model, under which the government would designate approved destination countries, before the DPDP Act settled on the negative-list structure it ultimately enacted.[38]

The Digital Personal Data Protection Act, enacted on 11 August 2023, abandoned the tiered architecture entirely.[39] Section 16 adopts the negative-list model Basu, Hickok, and Chawla had anticipated as India's most probable eventual landing point, and the USTR's 2024 National Trade Estimate Report characterised the shift as a positive development for market access.[40] Whether that characterisation captures what actually changed is the question the remainder of this Part addresses.

B. *The Sectoral Stack: Localisation That Survives the Act*

Section 30 of the DPDP Act preserves the operation of other laws governing personal data except where they directly conflict with the Act, which means the sector-specific rules built up over the preceding five years continue to impose their own localisation requirements independently of, and occasionally inconsistently with, the general statute.[41] The practical effect is a regulatory stack: whatever Section 16 provides, or fails to provide, sectoral rules layer additional constraints on top of it. Basu, Hickok, and Chawla's taxonomy captures the resulting dynamic precisely, describing a conditional or negative-list approach at the legislative level being quietly undermined by hard localisation requirements that persist at the sectoral level.[42]

The RBI's payments directive is the clearest instance. Section 30's savings clause preserves it in full; the DPDP Act does nothing to displace the categorical requirement that payment-system data be stored exclusively within India, a requirement that goes well beyond anything Section 16 itself demands and that, as noted above, has not been shown to be the least restrictive means of achieving its own stated objectives.[43]

SEBI's 2022 circular on cloud adoption operates differently but reaches a comparable outcome.

[38] Parsheera, *Cross-Border Data Flows*, supra note 3, at 15–16.
[39] DPDP Act, supra note 1.
[40] Basu, Hickok & Chawla, supra note 8; Office of the U.S. Trade Representative, supra note 5.
[41] DPDP Act, supra note 1, § 30.
[42] Basu, Hickok & Chawla, supra note 8.
[43] RBI Master Direction, supra note 31; Parsheera, *Questioning the Means and Ends*, supra note 10, at 12–16.

It requires that cloud service providers used by regulated entities consent to SEBI's supervisory oversight and that no foreign law impede that access.[44] The circular does not mandate Indian storage in terms, but its access conditions create practical pressure toward domestic storage or toward providers structured around Indian-law contractual frameworks, a pattern of functional localisation achieved through access conditions rather than an explicit storage mandate. Burri identifies this pattern as a significant source of regulatory fragmentation in comparative practice precisely because it is harder to identify, and harder to challenge, than an outright storage requirement.[45]

IRDAI's 2017 Guidelines on Information and Cyber Security for Insurers require that all policyholder data be stored and processed on infrastructure physically located in India.[46] These guidelines predate the DPDP Act and were never revisited following its enactment, leaving a parallel and unreconciled localisation requirement in place for the insurance sector, one whose tension with reinsurance arrangements, which by their nature transfer risk and associated policyholder data to international reinsurers, illustrates concretely the kind of incoherence the regulatory stack generates for firms operating under more than one regime at once.

The Telecommunications Act, 2023 introduces a "trusted source" framework for network equipment and services, sharpened by India's documented concerns about Chinese telecommunications infrastructure, most visibly the exclusion of Huawei and ZTE from 5G rollout, paired with localisation expectations for sensitive network and subscriber data.[47] Section 16's negative-list mechanism could in principle be used to formalise these technology-specific transfer restrictions, but the absence of statutory criteria for the negative list means there is currently no principled legal basis distinguishing a security-driven designation from one that serves industrial-policy or diplomatic ends.

C. *The 2025 Draft Rules: Localisation Returns Through the Back Door*

If the sectoral stack shows that localisation survived the DPDP Act's enactment, the Draft Digital Personal Data Protection Rules, 2025 show that it did not even stay confined to the

[44] Securities and Exchange Board of India, Circular on Cloud Adoption by SEBI Regulated Entities, CIR/CFD/CMD1/7/2022 (Feb. 10, 2022).
[45] Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Lego*, 51 U.C. Davis L. Rev. 65, 68–75 (2017).
[46] Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security for Insurers, IRDAI/IT/GDL/MISC/100/5/2017 (Apr. 11, 2017).
[47] Telecommunications Act, 2023, No. 44, Acts of Parliament, 2023 (India).

sectors that predate the Act. Rule 12(4) requires Significant Data Fiduciaries to ensure that specified categories of personal data, categories the Central Government is to identify on the recommendation of a committee, are not transferred outside India, a direct localisation requirement operating independently of the negative-list mechanism in Section 16 itself.[48] Malviya and Singh's analysis of the provision identifies the core problem clearly: there is no published criterion for which data categories will be restricted, no defined process for how the underlying committee will make that determination, and no advance notice mechanism by which a firm can know whether it will be designated a Significant Data Fiduciary in the first place.[49] Rule 14 compounds the uncertainty by granting the Central Government broad discretion to impose localisation obligations on any data fiduciary by notification, a power that, in their words, could function as a general enabling mechanism for localisation regardless of what Section 16's negative-list architecture appears to promise on its face.[50]

The comparison with the GDPR that Malviya and Singh draw is instructive. The GDPR's Chapter V mechanism is undeniably more prescriptive than a negative list, adequacy decisions, standard contractual clauses, binding corporate rules, but each instrument comes with defined criteria and a known procedural pathway.[51] A data fiduciary relying on standard contractual clauses knows what it needs to demonstrate. A Significant Data Fiduciary under the Draft Rules cannot know, in advance, which categories of data it holds might become subject to Rule 12(4), because the rule leaves that determination to a committee process the text does not describe. The Rules also leave what Malviya and Singh call the "onward transfer" gap unaddressed: once data lawfully leaves India for a permitted destination, Indian law has no mechanism for regulating what that destination does with it afterward, a gap the GDPR closes through its own onward-transfer principles but that the DPDP framework, Act and Draft Rules alike, does not.[52]

Taken together with the sectoral stack, the Draft Rules confirm this article's central claim more directly than the Act's text alone could. The negative-list model was never, on inspection, a complete answer to the localisation question; it was a placeholder that left the executive free to reintroduce category-based and entity-based localisation whenever it judged that necessary,

[48] Malviya & Singh, supra note 6 (discussing Rule 12(4) of the Digital Personal Data Protection Rules, 2025 (Draft)).
[49] Malviya & Singh, supra note 6.
[50] *Id.* (discussing Rule 14 of the Digital Personal Data Protection Rules, 2025 (Draft)).
[51] GDPR, supra note 19, arts. 45–47; Malviya & Singh, supra note 6.
[52] Malviya & Singh, supra note 6.

through instruments, delegated rules, sectoral circulars, that face considerably less legislative scrutiny than a statutory amendment would.

V. CRITICAL DISCUSSION

Three consequences follow from this arrangement, and they are worth separating because they operate on different actors and different timescales.

The first is a legal-certainty cost borne primarily by data fiduciaries and, less directly, by data principals who cannot easily know what protections travel with their data once it leaves the country. A negative list without criteria is not neutral as between openness and restriction; it is neutral only in the sense that it defers the choice to a future exercise of discretion that firms must price into their compliance planning today. That cost is not evenly distributed. Large multinational firms can absorb the uncertainty, and often the compliance overhead once a restriction does materialise, through legal and infrastructure resources that smaller Indian firms and startups do not have. The compliance-cost literature on localisation generally, the OECD's 30 to 60 per cent estimate among the more concrete figures available, suggests this asymmetry will widen as the sectoral stack and the Draft Rules layer additional, unpredictable obligations on top of the general statute.[53]

The second cost runs to India's international negotiating position. A future adequacy decision from the European Commission, the kind of instrument that would let personal data move from the EU to India without additional safeguards, requires a degree of legal predictability the current architecture does not supply. Schwartz's account of the "Brussels Effect" is instructive here: the EU's adequacy mechanism functions as much as a form of geopolitical leverage as a neutral legal standard, and jurisdictions seeking adequacy status have generally needed to demonstrate not just substantive alignment with GDPR-equivalent protections but procedural transparency in how transfer restrictions are decided.[54] An unreasoned, criteria-free notification power, reinforced by an equally unreasoned rule-making power under Rule 12(4), is a difficult foundation on which to build that case. Parsheera's account of India's trade diplomacy adds a further dimension: India's continued absence from the WTO's Joint Statement Initiative on E-commerce, its resistance to binding digital-trade commitments in the ongoing UK negotiations, and its observer status in the trade pillar of the Indo-Pacific Economic Framework all reflect a

[53] OECD, supra note 26.
[54] Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. Rev. 771, 798 (2019).

considered preference for preserving domestic regulatory space over accepting external discipline on data-flow questions.[55] Burri's "legal lego" analysis suggests that preference carries a cost of its own: the emerging multilateral data-governance framework will impose real compliance burdens on non-participants regardless of their formal abstention, and those costs are likely, over time, to exceed whatever flexibility staying outside the framework currently preserves.[56]

The third cost is domestic and constitutional in character, though a full doctrinal treatment of it lies outside this article's chosen scope. The Supreme Court's proportionality framework, developed in the original privacy judgment and confirmed as applicable to data-governance measures in the subsequent Aadhaar decision, asks whether a restriction on a fundamental right pursues a legitimate aim through the least restrictive means reasonably available.[57] A delegation of transfer-restriction authority that specifies no criteria for its own exercise sits uneasily with that standard, not because every exercise of the power will necessarily fail it, but because the absence of criteria makes it impossible to assess in advance whether a given restriction will satisfy the least-restrictive-means requirement or not. The RBI's payments directive already illustrates the risk directly: Parsheera's identification of workable, less restrictive alternatives, contractual access clauses, mutual legal assistance frameworks, real-time mirroring, means the directive's continued operation under Section 30's savings clause carries the same constitutional exposure it carried before the DPDP Act was enacted, an exposure the Act does nothing to resolve because it does not touch the sectoral instruments that generate it.[58]

What these three costs share is a common origin. Each traces back to the same design choice: a transfer-restriction power built to preserve maximum executive flexibility, at the expense of the statutory criteria, procedural transparency, and coordination across the sectoral stack that would make the power's exercise predictable, defensible, and internationally legible. That is not, on its own, evidence of bad faith or of a hidden intention to restrict trade under cover of liberalisation language. It is evidence of a regime built to keep options open, in a policy area where every other major jurisdiction, the EU through its adequacy architecture, China through

[55] Parsheera, *Cross-Border Data Flows*, supra note 3, at 17–19.
[56] Burri, supra note 46.
[57] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India); Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 SCC 1 (India).
[58] Parsheera, *Questioning the Means and Ends*, supra note 10, at 12–16.

its explicit hard-localisation statute, has chosen to close at least some of those options in exchange for predictability. India's choice not to close them is a legitimate strategic posture. Whether it is a sustainable one, given the costs identified above, is a separate question, and the answer depends substantially on whether the gaps this article has identified are closed before they compound further through instruments like the 2025 Draft Rules.

VI. RECOMMENDATIONS

Four reforms would move the current architecture toward genuine coherence without abandoning the negative-list model's basic structure, which remains, on balance, a defensible starting point provided its operation is made predictable.

1. *Statutory criteria for the Section 16 power.*

Section 16 should be amended to specify the factors the government must weigh before restricting transfer to a given destination: the destination's data-protection standards, the scope of government surveillance there, and the judicial remedies available to affected data principals, broadly the assessment structure the GDPR's Article 45(2) uses for adequacy determinations, adapted to the necessity standard Mattoo and Meltzer propose for reconciling privacy regulation with trade-law disciplines.[59] The resulting assessment should be published and tabled before Parliament with reasons, not issued as an unreasoned notification.

2. *Comparable criteria for Rule 12(4) and Rule 14.*

The same discipline should extend to the Draft Rules before they are finalised. The committee process contemplated for identifying restricted data categories under Rule 12(4) should operate under published criteria and a defined procedure, and Significant Data Fiduciary designations should carry advance notice sufficient to allow affected firms to plan their compliance posture, addressing directly the predictability gap Malviya and Singh identify.[60]

3. *Coordination of the sectoral stack.*

The Central Government should establish a coordinating body bringing together the RBI,

[59] GDPR, supra note 19, art. 45(2); Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 J. Int'l Econ. L. 769, 771–73 (2018).
[60] Malviya & Singh, supra note 6.

SEBI, IRDAI, the Department of Telecommunications, and the Data Protection Board to align localisation requirements across sectors rather than allowing them to accumulate independently of one another. Parsheera's analysis offers a workable template specifically for the RBI's payments directive: its stated supervisory objectives could be achieved through mandatory contractual access provisions and mutual legal assistance frameworks considerably less trade-restrictive than exclusive domestic storage, and the directive should be formally reassessed against the proportionality standard given how substantially India's domestic data-centre capacity has grown since 2018.[61]

4. ***A more active posture in multilateral data governance.***

India's long-term interest in capturing value from cross-border data flows is better served by shaping the emerging multilateral framework as a participant than by remaining outside it in the name of preserving flexibility. Engagement with the APEC Cross-Border Privacy Rules system as a route toward multilateral integration, together with formal adequacy consultations with the European Commission, would give India a stronger basis for negotiating the terms of that framework than continued absence from the WTO's Joint Statement Initiative currently provides.[62]

VII. CONCLUSION

The question this article set out to answer, whether the DPDP Act has produced a coherent cross-border transfer regime or has simply moved localisation authority from legislative text to executive discretion, has, on the evidence reviewed here, a fairly clear answer. Section 16's negative-list structure is formally more permissive than any of the frameworks India considered and rejected between 2018 and 2022, but that formal permissiveness coexists with, and is substantially qualified by, a sectoral stack the Act leaves untouched and a set of Draft Rules that reintroduce category-based localisation through delegated rule-making rather than statutory amendment. The RBI's payments directive, SEBI's cloud-access conditions, IRDAI's insurance guidelines, and the telecommunications trusted-source framework all continue to operate exactly as they did before August 2023, regardless of what the Central Government ever does or does not do with its Section 16 power. Rule 12(4) of the Draft Rules adds a further,

[61] Parsheera, *Questioning the Means and Ends*, supra note 10, at 12–16.
[62] Parsheera, *Cross-Border Data Flows*, supra note 3, at 17–19; Burri, supra note 46.

entity-specific localisation mechanism operating alongside, not through, that power.

None of this means India's underlying strategic posture, a deliberate middle path between the open data-flow model the United States has generally favoured and the closed, state-centric model China has adopted, is incoherent as a matter of policy. UNCTAD's developmental critique of unconditional liberalisation gives that posture real intellectual grounding, and there is nothing inherently unreasonable about a large developing economy wanting to preserve regulatory flexibility while its digital industry matures. What is missing is not the strategic judgment but the statutory architecture to make that judgment legible, defensible, and internationally credible. A negative list without criteria, reinforced by sectoral instruments the Act does not coordinate and Draft Rules that expand rather than narrow the executive's discretion, delivers flexibility for the government and uncertainty for everyone else. Closing that gap, through statutory criteria for Section 16, comparable discipline for the 2025 Rules, coordination across the sectoral regulators, and a more active role in shaping the multilateral rules India will eventually have to operate within regardless, is the unfinished work the DPDP Act leaves for whoever takes up its implementation next.