

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any **suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

The Law and Economics of Data Localisation in India: Efficiency, Market Failure and the Design of Cross-Border Data Governance

SHASHANK PATHAK* AND DR. A.B. DEBASIS ROUT**

ABSTRACT

This article examines the economic implications of data localisation for India through the lens of law and economics. It pursues three objectives: to reframe the localisation debate as a question of efficiency rather than of sovereignty, to determine the conditions under which a restriction on cross-border data flows is economically justified, and to propose a governance framework calibrated to those conditions. In method it is doctrinal and analytical, combining a positive analysis of the welfare effects of data governance with a normative assessment against the criterion of efficiency, and proceeding by a comparative institutional analysis of the principal cost studies and of the statutory, regulatory and treaty instruments of Indian data governance. On this approach, cross-border flows are a source of efficiency and positive externalities, so that a restriction imposes a deadweight loss justified only where it corrects a market failure, whether an externality or a concentration of market power, at a cost smaller than the harm it would otherwise produce. India is at once the leading exporter of data-intensive services and a major source of consumer data whose value is captured largely abroad, a tension the article calls the IT-BPM Paradox. Drawing on a sectoral analysis, the distributional critique of the United Nations Conference on Trade and Development and the disciplines of international trade law, it argues that neither comprehensive localisation nor unconditional liberalisation is efficient, and proposes a framework that selects, for each category of data, the least-cost instrument that addresses the market failure at stake.

Keywords: Data localisation, cross-border data flows, law and economics, Data Protection, proportionality.

* Author is a Research Scholar at National Law University Odisha, India.

** Author is an Assistant Professor (Accounts) at National Law University Odisha, India.

I. INTRODUCTION: THE ECONOMIC STAKES OF DATA GOVERNANCE

The economic analysis of data localisation is, in essence, an inquiry into cost and benefit, asking whether the restriction of cross-border data flows generates benefits, in domestic infrastructure investment, in the domestic capture of data value, and in regulatory effectiveness, sufficient to outweigh the costs of reduced trade competitiveness, higher compliance expenditure, and the loss of global digital efficiencies. In the Indian context the inquiry is strategically asymmetric, because India is at once a major net exporter of digital services, whose performance depends upon liberal cross-border flows, and a major source of consumer data processed predominantly by foreign-owned platforms in a manner that allows the value of that data to accrue outside India. This dual position is what the article calls the IT-BPM Paradox, and its resolution is the central problem of Indian data governance.

The approach taken is that of law and economics, combining a positive analysis of the incentive and welfare effects of data governance with a normative assessment against the criterion of efficiency, and asking in each case not whether a measure is desirable in the abstract but whether it attains its objective at a lower social cost than the alternatives.¹ The empirical foundation is supplied by four quantitative studies which, though differing in method and scope, converge upon the conclusion that localisation imposes significant costs. The European Centre for International Political Economy estimated, using a computable general equilibrium model, that economy-wide localisation would reduce India's income through its effect upon investment, technology transfer, productivity, and export competitiveness,² an estimate criticised by Carnegie India for resting upon static assumptions that cannot capture dynamic innovation effects.³ CUTS International assessed the welfare costs of localisation for India and identified the contraction of digital exports, higher domestic prices, reduced inbound investment, and lower productivity as the channels of loss,⁴ while the Information Technology and Innovation Foundation documented the same categories of cost across many jurisdictions without disaggregating them by economy,⁵ and the Organisation for Economic Co-operation and Development found, through an index of services trade restrictiveness, that greater

¹R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

²Erik van der Marel, Hosuk Lee-Makiyama & Matthias Bauer, *The Costs of Data Localisation: Friendly Fire on Economic Recovery* (Eur. Ctr. for Int'l Pol. Econ., ECIPE Occasional Paper No. 3/2014, 2014).

³Anirudh Burman & Upasana Sharma, *How Would Data Localization Benefit India?* (Carnegie India 2021).

⁴CUTS INT'L, *DATA LOCALISATION: INDIA'S DOUBLE-EDGED SWORD* (CUTS-CCIER 2020).

⁵Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them* (Info. Tech. & Innovation Found. 2021).

restrictiveness reduces traded output and economy-wide productivity.⁶ Each study, however, measures cost against a counterfactual of unrestricted flows that does not correspond to India's real choice, which lies among different designs of governance rather than between comprehensive localisation and complete liberalisation.

The analysis proceeds in five stages: the framework of law and economics, the IT-BPM Paradox, a sectoral analysis, the distributional critique within the disciplines of international trade law, and a framework for calibrating localisation across categories of data.

II. DATA ANALYSIS

A. The Analytical Framework of Law and Economics

The framework of law and economics evaluates a rule by its effect upon aggregate welfare and treats a restriction upon private activity as justified only where it corrects a market failure at a cost smaller than the harm the failure would otherwise produce. Cross-border data flows are a source of efficiency, because they allow data to be processed wherever this can be done at least cost and they generate positive externalities through network effects, technology diffusion, and the productivity of data-dependent industries, so that a restriction upon them imposes a deadweight loss that must be justified. Only two grounds supply that justification. The first is an externality that private contracting cannot internalise, as where processing abroad exposes the data subject or the state to a risk of compelled foreign access that no contractual term can exclude. The second is a concentration of market power, as where processing is dominated by a few platforms that capture most of the value the data generates. Where neither is present a restriction reduces welfare without curing any failure, and where one is present the efficient response is the instrument that addresses it at the lowest social cost rather than the most restrictive instrument available. A neglected element of the framework is the cost of uncertainty itself, because an inability to predict how a discretionary power will be exercised raises the transaction costs and the risk premium attaching to investment, so that an unpredictable regime may cost as much as an explicit restriction.

B. The IT-BPM Paradox: India as Exporter of Data Services and Claimant of Data Sovereignty

India's information technology and business process management sector is the most significant structural feature of its digital economy, generating revenues very large in relation to national

⁶Carlotta Del Giovane, Janos Ferencz & Javier López González, *The Nature, Evolution and Potential Implications of Data Localisation Measures* (OECD Trade Policy Paper No. 278, 2023).

income, employing several million persons, and supplying a substantial share of exports and of the foreign exchange that sustains the external account.⁷ Its dependence upon cross-border flows is structural, because its business model is the remote delivery of services to clients in the United States, Europe, and the United Kingdom, which requires the movement of client data across borders as an inherent condition of operation. A requirement that client data be stored within the client's jurisdiction would be incompatible with the offshore model on which much of the sector's revenue depends, and even a lesser requirement would raise costs by compelling providers to operate infrastructure in several jurisdictions and so fragment the economies of scale that make the Indian model competitive.⁸

The paradox is the tension between the assertion of data sovereignty through localisation and India's interest as the leading exporter of data-intensive services, which depends upon the very freedom that localisation restricts. The Srikrishna Committee sought to manage it through a graduated regime mirroring sensitive data and treating a narrow category of critical data more strictly,⁹ and the Digital Personal Data Protection Act of 2023 resolved it provisionally in favour of the commercial interest by abandoning mandatory localisation in favour of a mechanism that permits transfer by default and restricts it only to countries the Central Government notifies.¹⁰ Whether that resolution is efficient depends upon how the power of restriction is used, because frequent and uncriterial-based resort to it would generate uncertainty equivalent in effect to a localisation mandate. The deeper lesson is that the paradox rests upon a failure to distinguish the inbound flow of foreign client data, which is the sector's comparative advantage, from the outbound flow of the personal data of Indian residents, which is the proper object of sovereignty concern, so that a restriction broad enough to address the latter may needlessly impair the former.

C. Sectoral Analysis

India's longest experience of localisation is in digital payments, where the Reserve Bank of India has since 2018 required that payment system data be stored only within the country, and the assessment is contested.¹¹ Defenders argue that it stimulated domestic data-centre investment, enabled supervision without dependence upon foreign cooperation, and supported

⁷NASSCOM, STRATEGIC REVIEW: TECHNOLOGY SECTOR IN INDIA (2025).

⁸NASSCOM, STRATEGIC REVIEW: IT-BPM SECTOR IN INDIA 2019: DECODING DIGITAL (2019).

⁹COMM. OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS (2018).

¹⁰The Digital Personal Data Protection Act, 2023, § 16, No. 22 of 2023, Acts of Parliament, 2023 (India).

¹¹RESERVE BANK OF INDIA, STORAGE OF PAYMENT SYSTEM DATA, Notification No. RBI/2017-18/153 (Apr. 6, 2018).

indigenous payments infrastructure. Critics reply that it imposed substantial compliance costs upon the international card networks, part of which was shifted forward to Indian merchants and consumers, impeded cross-border interoperability, and weakened global fraud-detection systems, which are a network good whose value falls when the data is fragmented by jurisdiction.¹² The balanced view is that the experience is ambiguous, because the compliance costs were real, the infrastructure gains were real but concentrated as rents to domestic operators, and the supervisory benefit could in most respects have been secured by the less restrictive expedient of requiring the regulated entity to furnish data upon lawful demand rather than store it locally.

Within outsourcing, the services most sensitive to governance are cloud infrastructure services, whose value lies in provisioning resources wherever they are cheapest so that domestic-storage rules would force a costly restructuring, and the processing of health, financial, and personnel records, which depends upon the cross-border movement of exactly the data that attracts heightened scrutiny. The Act permits transfer by default, but the absence of an adequacy recognition in India's favour under the European framework leaves providers serving European clients reliant upon contractual mechanisms of uncertain sufficiency.¹³ Healthcare adds a further tension, since integrating Indian health data into global research requires cross-border flows while the sensitivity of the health information of more than a billion persons argues for caution, and the OECD literature suggests that localisation raises the cost of cross-border clinical trials and of advanced manufacturing appreciably, even as the concentration of sensitive data in domestic infrastructure itself creates a high-value target whose breach would expose very large numbers of records.¹⁴

D. The Distributional Critique and the Discipline of International Trade Law

The aggregate estimates assume that free flows are themselves optimal and measure localisation as a departure from that optimum. The United Nations Conference on Trade and Development contests this by asking who captures the value that flows generate, describing a pattern in which a developing economy exports raw data to be processed and monetised by foreign platforms and imports the value-added services they produce, reproducing the asymmetry between exporters of primary commodities and of manufactured goods.¹⁵ Properly understood this is a

¹²Burman & Sharma, *supra* note 3.

¹³Regulation 2016/679, art. 45, 2016 O.J. (L 119) 1 (EU).

¹⁴Del Giovane, Ferencz & López González, *supra* note 6.

¹⁵U.N. CONF. ON TRADE & DEV., DIGITAL ECONOMY REPORT 2021: CROSS-BORDER DATA FLOWS AND DEVELOPMENT (2021).

problem of market power, because processing is concentrated in a few platforms entrenched by the switching costs that users face, and the efficient response is to attenuate that power through obligations of portability and data sharing and the taxation of the resulting rents rather than to relocate the data, instruments the Indian non-personal-data framework had begun to examine before it was set aside.¹⁶

The critique also clarifies the paradox, because the flow that generates the distributional concern is the outbound flow of the personal data of Indian residents while the flow that sustains the export sector is the inbound flow of foreign client data, so that a regime confined to the former leaves the latter undisturbed, and India's very large base of data subjects is better deployed as negotiating leverage for equitable terms of participation than in costly localisation.

India's choices are constrained by the General Agreement on Trade in Services, whose Article XIV permits otherwise inconsistent measures necessary to protect the privacy of individuals in the processing of personal data, the operative term being necessity.¹⁷ As the Appellate Body of the World Trade Organization has explained, necessity is not indispensability but a weighing of the importance of the objective, the contribution of the measure, and its trade-restrictiveness, with a reasonably available less restrictive alternative forming part of the analysis, which is in economic terms a requirement to select the least-cost instrument capable of attaining the objective.¹⁸ This aligns with the proportionality standard of Indian constitutional law, under which a measure must pursue a legitimate aim, be rationally connected to it, be the least intrusive means, and strike a fair balance, so that a measure failing the constitutional test is likely also to fail the necessity test.¹⁹ Applied to the Act, the negative-list mechanism is defensible as a framework, and the vulnerability lies in the exercise of the restriction power, since a broad and criteria-less restriction would be difficult to defend as either proportionate or necessary, a point of practical weight in the free trade negotiations with the European Union, the United Kingdom, and the United States in which India's market access depends upon showing that its framework satisfies the substantive objectives of data protection.²⁰

E. A Framework for Calibration and the Burden upon Small Enterprises

¹⁶MINISTRY OF ELECS. & INFO. TECH., REPORT BY THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK (2020).

¹⁷General Agreement on Trade in Services art. XIV(c)(ii), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183.

¹⁸Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R (Apr. 7, 2005).

¹⁹K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).

²⁰Svetlana Yakovleva & Kristina Irion, *Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade*, 10 INT'L DATA PRIVACY L. 201 (2020).

Taken with the proportionality standard, the analysis yields an efficiency test. A localisation measure is justified only where it serves an objective corresponding to a genuine market failure, where localisation is genuinely connected to correcting that failure, where no less restrictive instrument would do, where its scope is confined to the data the objective requires so that no needless deadweight loss is imposed, and where its benefit exceeds its cost. The test yields different results for different data. Data relating directly to national security satisfies it, because the objective is weighty and contractual protection is defeated where a foreign sovereign can compel disclosure regardless of the place of storage, so that localising a narrow security-critical category is the efficient instrument.²¹ Consumer financial data is intermediate, because supervision and fraud detection are legitimate but physical storage is not the least-cost means of attaining them when production upon lawful demand would suffice, the distinction being that between a property rule, which protects the entitlement by prohibiting disturbance, and a liability rule, which permits disturbance against compliance with a standard.²² General consumer data fails the first condition, because no market failure requires its domestic storage rather than strong processing obligations and conditional transfer, and localising the great majority of platform data would impose a very large deadweight loss, so that the Act's negative-list default is the efficient treatment.

A further consideration that the aggregate estimates obscure is the disproportionate burden of compliance upon micro, small, and medium enterprises, which account in India for a large share of income, exports, and employment. Because the fixed overheads of compliance are largely indivisible, they generate economies of scale in compliance and fall far more heavily, as a share of revenue, upon a small firm than upon a large one, so that a uniform obligation operates as a barrier to entry that favours incumbents.²³ The Act provides no reduced pathway, applying the same obligations to a micro-enterprise and to a major corporation, a uniformity that is inefficient and inequitable, and a regime calibrating obligation to the volume and sensitivity of the data processed, building upon the Act's significant-data-fiduciary distinction, would align private compliance cost with marginal social harm.²⁴ The European framework already exemplifies such calibration in its lighter obligations upon smaller organisations.²⁵

²¹Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018).

²²Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

²³CUTS Int'l, *supra* note 4. See also George J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. SCI. 3 (1971).

²⁴The Digital Personal Data Protection Act, 2023, §§ 10, 17, No. 22 of 2023, Acts of Parliament, 2023 (India).

²⁵Regulation 2016/679, art. 30(5), 2016 O.J. (L 119) 1 (EU).

III. CONCLUSION

The article set out to assess data localisation in India as a question of efficiency rather than of sovereignty, asking in each case whether restricting cross-border flows corrects a market failure at a cost smaller than the harm it would otherwise produce. The evidence and the analysis converge upon a single answer, because the quantitative studies show that localisation imposes real costs, the framework explains why those costs take the form of deadweight loss and elevated transaction costs, and the sectoral and distributional analysis shows that the gains localisation is meant to secure are modest, concentrated, or attainable by less restrictive means. Neither comprehensive localisation nor unconditional liberalisation is therefore efficient for India, and the IT-BPM Paradox dissolves once the inbound flow of foreign client data is distinguished from the outbound flow of the personal data of Indian residents, because a regime restraining only the latter pursues the sovereignty interest without sacrificing comparative advantage.

Five principles follow. The regime should differentiate by the market failure at stake, ranging from the localisation of a narrow national-security category, through regulatory access for financial data, to conditional transfer for general consumer data. The intensity of compliance obligation should track marginal social harm, because a uniform obligation burdens small enterprises without proportionate benefit and deters entry. The comparative advantage of the export sector should be protected structurally against the localisation of, or uncertainty over, the client data it processes. The distribution of data value, being a problem of platform market power, should be addressed through portability, data sharing, and taxation rather than through localisation. And regulatory certainty should be treated as itself a determinant of efficiency, because unpredictability in the exercise of the restriction and exemption powers raises the transaction costs of investment.

Read together, these principles answer the question with which the article began, because the efficient course for India is neither to localise comprehensively nor to liberalise without condition but to calibrate, selecting for each category of data the least-cost instrument that corrects the market failure at stake and embedding that calibration in a regime whose predictability is itself a source of efficiency. The negative-list architecture of the Digital Personal Data Protection Act supplies a defensible foundation for that course, but it will deliver the efficiency its design makes possible only if the discretion it confers is disciplined by published criteria, by independent assessment, and by periodic review.

IV. RECOMMENDATION

India should decline to adopt comprehensive localisation, which the evidence shows to be inefficient, and should instead adopt a calibrated framework organised around the data category and the market failure at stake. The strictest storage requirement should be confined to a narrow class of national-security data, where contractual protection against compelled foreign access fails. The supervisory aims of the financial sector should be met by requiring the production of data upon lawful demand rather than physical storage, which would permit a reconsideration of the payments-sector rule. General consumer data should remain under the Act's default of permitted transfer, with the restriction power disciplined by published criteria, by prior assessment of the economic and rights-related consequences of any restriction, and by periodic review. The client data processed by information technology and business process management providers should be exempted from domestic-storage requirements subject to contractual standards, and a graduated compliance pathway should relieve the low-risk processing of small enterprises of disproportionate obligations. The distribution of data value should be pursued through obligations of portability, through data-sharing obligations upon dominant platforms, and through the taxation of data-derived rents. Above all, India should treat regulatory predictability as a central determinant of efficiency and deploy the scale of its data-subject population as leverage for equitable participation in the global data economy rather than for the defensive restriction of data flows.
