Cross-Border Data Flows and India's Digital Sovereignty

India's Draft Data Protection Rules

Akriti Gaur

12.03.2025 doi: 10.59704/82a368a8a6158abf

India's data protection framework has been in the making for over a decade. The Digital Personal Data Protection Act ("DPA") was passed by Parliament in 2023,[1] and the draft Digital Personal Data Protection Rules ("draft Rules") were released in January 2025 for public consultation. While the DPA is the parent legislation for rights, duties, and obligations in the domain of personal data protection, it authorizes executive rule-making by the Central Government to flesh out guidelines to implement key provisions of the Act. Accordingly, the draft Rules provide operational instruction for Data Fiduciaries, Data Principals, state agencies and other intermediaries. However, among other things, the draft Rules have been criticized for failing to articulate a mechanism for data breach notifications, as well as for the collection and verification of children's consent. Further, longstanding concerns about the Data Protection Board's independence and impartiality remain unaddressed. Crucially, the draft Rules are vague on how users can enforce rights outlined in the parent legislation.[2]

In this piece, I argue that the draft Rules do little to clarify India's murky position on cross-border data flows. The ambiguous wording of the text grants unfettered discretion to the executive in operationalizing the localization mandate. Moreover, the lack of legislative protections for citizen privacy, coupled with missed opportunities to establish robust institutional frameworks undermines India's own data diplomacy project.

Legislative history

For a long time, the Indian Government has remained uncertain about its stance on cross-border flows of personal data. While lawmakers have been consistent in their commitment to achieve "data sovereignty,"[3] the path to achieving this remains unclear. In the past, the Government has proposed or implemented similar commitments in other sectors,[4] but a holistic policy on regulated cross-border flows has been mired in controversy. For instance, in a proposed legislation preceding the DPA, the Draft Personal Data Protection Bill, 2018 proposed by the Justice B.N. Srikrishna Committee,[5] all Data Fiduciaries were required to "localize" personal data within the Indian territory.[6] These entities were mandated to maintain a "serving copy" of personal data on servers or data centers located in India. The Bill empowered the Government to declare certain categories of personal data as "critical personal data" for exclusive localization, i.e. where cross-border transfer or processing would be completely prohibited. This and subsequent iterative proposals of conditional localization mandates faced substantial criticism. Scholars, civil society, and industry experts have been skeptical of the stated benefits for national security and law enforcement and boosting homegrown initiatives, among other things.

DPA's vague cross-border flow provision

In 2023, the DPA made it clear that Data Fiduciaries can transfer personal data to other countries, with

[1] The Digital Personal Data Protection Act ("DPA") https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[2] Jhalak M. Kakkar & Shashank Mohan, *How the draft rules for implementing data protection falls* short, The Hindu, January 13, 2025; https://www.thehindu.com/sci-tech/technology/how-the-draft-rules-for-implementing-data-protection-falls-short/article69092017.ece

[3] Read along with "data protectionism", "data nationalism", "data exceptionalism" – where states seek to maintain control over personal data of their citizens/residents, rindrajit Basu, Elonnai Hickok,andAditya Singh Chawla, The Localisation Gambit – Unpacking Policy Measures for Sovereign Control of Data in India, The Centre for Internet Society, March 19, 2019, https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

restrictions only if a particular jurisdiction has been "notified" by the Central Government as a restricted jurisdiction.[7] However, this provision is drafted broadly and does not specify the nature and sensitivity of personal data that would be restricted. The DPA does not provide any legislative guidance to the Government when determining a restricted jurisdiction.

Rule 14 of the draft Rules creates further uncertainty. Transfers of personal data processed in India or belonging to Data Principals residing in India shall be subjected to "requirements" laid down by the Central Government. However, neither the DPA nor the draft Rules clarify the nature or scope of these potential restrictions. Moreover, Rule 12(4) of the draft Rules sneaks in a significant departure from the DPA by bringing back exclusive localization of personal data specified by the Central Government for Significant Data Fiduciaries, based on the recommendation by a committee. Again, the draft Rules remain silent on the scope and objectives of such categorization and recommendation.

Data autonomy or sovereignty has become a priority for national governments but can be a "double-edged sword" if implemented in the absence of guardrails to check state power.[8] While regulation of cross-border personal data flows has become a consistent feature of emerging national data protection legislation,[9] many legislations incorporate clear guidelines to prevent arbitrary decision-making. The EU General Data Protection Regulation (GDPR), for instance, lays down adequate guidelines for regulators to decide on the nature and scope of regulating data transfers.[10] It outlines specific conditions for making such "adequacy" assessments, including whether the recipient country upholds respects the rule of law and human rights through domestic and international commitments, and whether it has an independent supervisory authority to enforce the data protection framework.[11] By contrast, India's widely drafted provisions grant considerable discretion to the executive, leaving decisions susceptible to shifting political objectives, and quite possibly bilateral or multilateral relations. Further, the complete absence of legislative guidelines creates a fair amount of legal and operational uncertainty for Data Fiduciaries and Principals alike. Globally, decisions on cross-border flows are made on the basis of "reciprocity", "adequacy" or the presence of "comparable safeguards".[12] These factors are typically outlined in data protection legislation in varying degree. The DPA read with the draft Rules is silent on these considerations leaving the executive with unchecked power to make such decisions.

Data diplomacy - a two-way street

What does this vague cross-border flow mandate mean for India's own data diplomacy project? The Government will have to consider this when the framework comes into effect. Aside from the indeterminate phrasing, there is a lot more that the government will have to consider when it finds itself on the other side of an adequacy assessment. For instance, the DPA provides wide exemptions to the Indian Government to process personal data.[13] This all-encompassing escape clause for the state serves a serious blow to other well-meaning safeguards outlined in the law. Further, the current covert surveillance framework is not authorized by legislation or independent oversight.

[4] Id.
[5] The Personal Data Protection Bill, 2018, https://prsindia.org/files/bills_acts/bills_parliament/1970/Draft%20Personal%20Data%20Protection%20Bill,%202018%20Draft%20Text.pdf
[6] Sections 40 and 41, Personal Data Protection Bill, 2018.
[7] Section 16, DPA [Processing of personal data outside India].
[8] Anupam Chander and Haochen Sun, "Sovereignty 2.0" (2021). Georgetown Law Faculty Publications and Other Works. 2404. https://scholarship.law.georgetown.edu/facpub/2404/
[9] UNDP Guide – Drafting Data Protection Legislation – A study of regional frameworks (2023), https://www.undp.org/sites/g/files/zskgke326/files/2023-04/UNDP%20Drafting%20Data%20Protection%20Legislation%20March%202023.pdf ("UNDP Guide").
[10] Article 45, GDPR.
[11] Article 45 (2), GDPR.
[12] UNDP Guide at p. 146.
[13] Section 17, DPA.

Further, scrutiny has been directed at the composition and independence of the Data Protection Board, adding to doubts about India's position as a serious player in multilateral and bilateral personal data-sharing. Typically, when a receiving nation is not "deemed adequate"[14] based on reciprocity of safeguards, bilateral data-sharing arrangements can be executed. However, even in these cases, India will have to be careful about scrutiny into its own domestic data protection deficiencies. For instance, a key concern for the Schrems litigation in Europe has been the US surveillance regime and general uncertainty about the regulatory landscape surrounding it.[15]Current adequacy decisions and their review documents indicate how the US surveillance regime continues to be a big cause for concern under the GDPR framework.[16] India will likely face similar and more pronounced challenges when it is on the other side of an adequacy assessment.

With the draft Rules, India is a step closer to becoming a serious global participant in multilateral and bilateral data protection processes. Its objective to boost a homegrown data industry is under scrutiny, as are its domestic privacy concerns. The current regulatory approach risks hindering reciprocity from other nations and weakening India's credibility in the global data economy. The draft Rules prove that the Government is still committed to a restrictive approach to cross-border data flows. However, it must not only address concerns of arbitrariness and uncertainty but also critically examine its own role in undermining citizens' privacy rights.

ABOUT THE AUTHOR

Akriti Gaur

Akriti Gaur is a Fellow at the Berkman Klein Center for Internet and Society at Harvard University. She is an Affiliate Fellow at the Information Society Project, Yale Law School and a Fellow at the Mass Atrocities in the Digital Era (MADE) program at Yale University. She researches and writes on AI governance, human rights, and regulation of emerging technologies.

SUGGESTED CITATION

Gaur, Akriti: Cross-Border Data Flows and India's Digital Sovereignty: India's Draft Data Protection Rules, Verfassungsblog, 12.03.2025, doi: 10.59704/82a368a8a6158abf.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20250313-001116-0.

[14] UNDP Guide at p. 148.

[15] The first Schrems case was filed against Meta (formerly Facebook) for violating the EU data protection framework by transferring data to US [ruled in Schrems favour], the second data protection framework was also about Facebook and the EU-US privacy shield (which took over from the safe harbour).

[16] See for instance, Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj