



This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

India's Cloud Computing dilemma: Data Residency vs Data Sovereignty

Mansi Dadhich

ABSTRACT

India doesn't have a cloud computing law. What it has instead is RBI circulars and the DPDP Act, patched together, and neither actually settles who controls your data once it's stored. This paper untangles three ideas that keep getting collapsed into one: residency, localisation, and sovereignty. Data can sit on a server in Mumbai and still be reachable by a foreign government, because the company running that server answers to its own country's laws first. The US CLOUD Act makes this obvious: AWS Mumbai stores Indian data, but AWS is American, so American law enforcement can still ask for it. RBI's 2025 NBFC directions are the first Indian rule to name sovereignty directly, tying it to who holds the encryption keys rather than where the hardware sits. It's a start. It just hasn't left banking yet.

BLOG

Is your data as secure as you think it is? The company handling your data (the data fiduciary) may store it physically in India, while the actual backend operations are handled by a foreign parent company. For decades, India has had no specialised laws governing cloud computing; regulatory oversight comes piecemeal from RBI mandates and the DPDP Act. According to RBI regulations, data stored in India stays in India, but is it as simple as it looks? Do foreign agencies have no access to data stored in India? Knowing this gap means separating three ideas: data residency, localisation, and sovereignty, which often get treated as one.¹

The first key of the triad is residency, where your data resides. Localisation is the legal requirement that data should be stored within a specific jurisdiction; India, in this case. Sovereignty, finally, means real control: who holds the encryption keys, who has administrative

¹ Divyansh Godara & Pragya Bhadana, *The Mirage of the Server: Analysing the Conflict between Indian Data Sovereignty and Extraterritorial Cloud Laws*, SCC Online Blog (June 27, 2026), <https://www.sconline.com/blog/post/2026/06/27/india-data-sovereignty-us-cloud-act-analysis/>.

access, and who is legally accountable for the data, regardless of where it lives physically. Cloud computing is essentially outsourcing; smaller enterprises rent computing resources and software from large providers instead of building their own infrastructure.² This provides them with leverage as it is cheaper and more sustainable. Even when data resides in India and localisation requirements are met, the cloud provider, as the actual owner of the software, still has visibility into it. This visibility gap, a provider having access to data that it legally doesn't own, is squarely where sovereignty breaks down, though the requirements of residency and localisation are fulfilled.

This is the gap that RBI's regulations and the DPDP Act's provisions attempt to close by governing both data fiduciaries and the cloud providers (sources) they rely on. Section 16 of DPDP Act reads that the Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.³ This statement in itself holds the key to securing the localisation of data. According to section 16, it grants the government the power to restrict where personal data leaves India, but it does not address who controls this data within India. That question, control not location, lies within the ambit of sovereignty, a gap this section leaves untouched. The mandates from RBI 2018 specify: All system providers shall ensure that the entire data relating to payment systems operated by them is stored in a "system only in India".⁴ This provision still stays bounded with localisation; the sovereignty question remains. The RBI's 2025 NBFC Outsourcing Directions (¶53(vi)-(vii), ¶94)⁵ go beyond storage requirements and expressly prohibit a foreign regulator or court from asserting jurisdiction over Indian operations based on offshore processing. This is Indian law naming the residency-sovereignty gap directly, not just mandating a server's location. With all the mandates mentioned, it still feels incomplete as every one of them is trying to govern their own slice.

On the contrary, when we look at the US CLOUD Act (2018), it takes the opposite approach: it allows a US-based company to cooperate with US law enforcement to hand over data it controls, regardless of where it was physically stored. The company matters more to the

² Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, Nat'l Inst. of Standards & Tech., Special Publication 800-145, at 2 (Sept. 2011), <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>.

³ The Digital Personal Data Protection Act, 2023, § 16, No. 22, Acts of Parliament, 2023 (India).

⁴ Reserve Bank of India, Storage of Payment System Data, RBI/2017-18/153, DPSS.CO.OD.No.2785/06.08.005/2017-2018 (Apr. 6, 2018).

⁵ Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025, RBI/DOR/2025-26/363, DOR.ORG.REC.No.282/21.04.158/2025-26, ¶¶ 53(vi)–(vii), 94 (Nov. 28, 2025).

authorities than the server. Take AWS Mumbai centre as an example: because AWS is headquartered in the US, it must comply with the CLOUD Act ⁶and hand over data whenever the US government demands it. The same AWS Mumbai centre that operates in India fulfils the location-based criteria, so Indian laws should govern. But the CLOUD Act doesn't recognise this location-based logic; it lets US jurisdiction reach the data anyway, regardless of where the server sits. India's counter-move relies on the RBI's 2025 NBFC Outsourcing Directions (¶97(v)(c)), which requires cloud governance policies to "ensure compliance with regulatory requirements, including those on privacy, security, **data sovereignty**, recoverability, and data storage requirements", ⁷and specifically mentions data sovereignty focusing on actual control. Notably, this is the first time a regulation explicitly names data sovereignty, moving the focus from just data storage. Going further, the RBI'S 2025 NBFC Outsourcing Directions(¶97(vii)(b)) require cloud architecture to provide "secure container-based data management, where **encryption keys and Hardware Security Modules are under the control of the NBFC**"; ⁸this stands to be the exact mechanism that determines whether a foreign government can compel access at all. This suggests that the Indian regulations are focused on defining sovereignty by control rather than just storage, even if so far done only with one financial segment.

India is not behind this first step towards acknowledging the difference of sovereignty and locality, which marks a real milestone, though there is a lot to be done. But this recognition hasn't been applied horizontally; the gap persists in all other sectors except this one. India still lacks a single regulatory body whose mandates should be generalised, covering data sovereignty across all sectors, not just finance. This matters even more when India is on its renowned path of 'Aatmanirbhar Bharat' (self-reliant India); ⁹The real self-reliance in a data economy means controlling data, not just storing it. As India positions itself as not just a hub for cheap labour but for advanced AI and tech infrastructure, a shift reflected in its role as co-architect of global AI governance norms at the 2026 India-Nordic Summit in Oslo¹⁰, Its regulations need to catch up with this reality, advancing towards genuine sovereignty, not just

⁶ Idts

⁷ Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025, RBI/DOR/2025-26/363, DOR.ORG.REC.No.282/21.04.158/2025-26, ¶ 97(v)(c) (Nov. 28, 2025).

⁸ *Id.* ¶ 97(vii)(b).

⁹ Press Information Bureau, Government of India, *Finance Minister Announces Government Reforms and Enablers Across Seven Sectors under Aatma Nirbhar Bharat Abhiyaan*, PIB Delhi (May 2020), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1624661>.

¹⁰ *India–Nordic Summit 2026 Signals Shift in Global AI Ruling Power*, IBC World News (May 21, 2026), <https://ibcworldnews.com/2026/05/21/india-nordic-summit-signals-shift-in-global-ai-ruling-power/>.

residency. The question isn't whether India can store its data at home; it already can. The question is whether it can own it fully.