HSR London International Conference on Multidisciplinary Academic Research
(HSR-ICMAR) 2026
https://houghtonstreetreview.com/index.php/conference

DATA LOCALIZATION REQUIREMENTS FOR PAYMENT SERVICE PROVIDERS: UZBEKISTAN AND INDIA

Rajesh Gajjar
National Forensic Sciences University, India
Tashkent State University of Law, Uzbekistan

Islombek Abdikhakimov
Under the Supervision of Dr

Abstract

When I first began mapping out possible dissertation directions, I was drawn less by an abstract interest in data protection law and more by a very concrete pattern I kept noticing at the intersection of Uzbek and Indian regulatory structures. In almost every conversation involving fintech, payments, or cross-border trade facilitation, the same question surfaced: where does the data physically sit. Clients want to know whether their payment data can sit on a server in Singapore or Frankfurt, or whether Indian law forces them into a domestic footprint. That recurring, very practical question is what convinced me this was worth a dissertation rather than a passing case study.

Uzbekistan entered the picture naturally, given the dual-degree structure with Tashkent State University of Law, but the pairing turned out to be more than administratively convenient. India and Uzbekistan are both states actively legislating around data sovereignty while trying not to choke off the very digital investment they are courting. Comparing a mature, high-volume digital payments ecosystem like India's with a smaller, rapidly modernizing one like Uzbekistan's gave me a genuine comparative tension to work with, rather than two jurisdictions that simply mirror each other.

Sitting With the Global Backdrop First

Before narrowing into the two case studies, I found it useful to sit with the wider picture. A meaningful share of countries worldwide now maintains some form of data protection law, and a substantial minority go further and mandate localization outright, feeding a compliance industry now worth tens of billions of dollars globally. What struck me is how rarely the justification for localization is purely technical. Governments invoke data sovereignty, cybersecurity, and economic development almost interchangeably, and the payments sector sits squarely at the intersection of all three, because transaction data is simultaneously personal, financial, and strategically valuable. That reframing changed how I read everything that followed: I stopped treating localization mandates as an inconvenience and started reading them as an expression of a state's claim over its own economic infrastructure.

India: A Framework Built in Layers

India's regulatory history reads like a series of responses to specific anxieties rather than a single coherent plan. The Information Technology Act, 2000 laid the earliest groundwork, with Section 43A introducing a general obligation to maintain reasonable security practices for sensitive personal data, but saying nothing about where that data had to live. The real turning point came in 2018, when the Reserve Bank of India issued its circular on storage of payment system data, requiring that the entire payments data of Indian users be stored exclusively within India, with no permanent mirroring abroad. That circular predates India's general data protection statute by five years, which tells me something

about sequencing: the RBI judged the payments sector too systemically important to wait for a horizontal privacy law, and moved first and narrowly.

Only in 2023 did the Digital Personal Data Protection Act fill the general gap, backed by penalties up to two hundred fifty crore rupees for material non-compliance, alongside CERT-In directions requiring critical infrastructure operators to retain system logs domestically for a rolling one-hundred-eighty-day period. Suspension of payment gateway access and licence cancellation are existential penalties, which tells me the RBI mandate functions less like one compliance item among many and more like a precondition for continuing to operate in India at all, applying across aggregators, gateways, banks, NBFCs, prepaid instrument issuers, and remittance providers.

Uzbekistan: A Framework Built Outward from Personal Data

Uzbekistan's trajectory runs in something close to the opposite direction, and reconstructing that sequence was one of the more rewarding parts of the research. The Law on Personal Data (No. ZRU-547 of 2019) established the foundational requirement that personal data of Uzbek residents be collected, processed, and stored on servers within the Republic, situated within the broader "Digital Uzbekistan 2030" strategy. Only after that foundation was in place did sector-specific obligations follow: the Law on Electronic Commerce extended domestic storage to e-payment and digital contract records, the Central Bank's Regulation on Payment Systems required national payment system operators to keep transaction data resident domestically, and the Cybersecurity Law of 2023 classified payment networks as Critical Information Infrastructure subject to mandatory audits.

What I take from this ordering is that Uzbekistan treated localization as a foundational principle of its digital economy from the outset, rather than as a payments-specific emergency measure the way India did. The five-year minimum retention period for transaction logs, the real-time reporting link to the State Tax Committee, and the requirement to use GOST cryptographic standards rather than internationally interoperable protocols all point toward a regime concerned with sovereign control over the entire data lifecycle. The enforcement path is also harsher in one respect: alongside fines and license revocation, Uzbekistan's framework allows criminal liability on repeated violations, a harder escalation than anything in the Indian structure. A layer I had not anticipated was how data handling increasingly intersects with an emerging Islamic finance conversation in Uzbekistan's central bank discussions on digital inclusion, suggesting any mature framework will eventually need to accommodate Sharia-compliant products as well.

What the Comparison Actually Teaches

Placing the two frameworks side by side is a useful device, but the real insight comes from where they diverge rather than where the categories line up. Both countries restrict cross-border transfers and require regulatory approval to move data out; both currently lack EU adequacy recognition; both attach severe penalties to non-compliance. But the institutional architecture differs meaningfully. India splits oversight across the RBI, MeitY, and CERT-In, meaning a PSP may need to satisfy three distinct authorities simultaneously. Uzbekistan concentrates authority more heavily in the Central Bank alongside the State IT agency, which should in principle produce a more coordinated compliance experience, though a less mature institutional ecosystem can introduce its own uncertainties.

The national payment-scheme architecture is another genuine point of divergence: India's Unified Payments Interface and the broader National Payments Corporation of India ecosystem, against Uzbekistan's Uzcard and Humo networks and the Uzbekistan Interbank Settlements system. This matters more than it first appears, because a domestic payment rail is not merely infrastructure, it is also a data-control mechanism. Routing transactions through a national scheme gives the regulator direct visibility that a foreign payment network lacks by default, which is presumably why India's framework requires networks such as Visa and Mastercard to replicate data domestically rather than

prohibiting their operation outright: the state wants both the presence of global rails and full sovereign visibility into the data they generate.

Where the Research Got Genuinely Difficult

Comparative work between a well-documented jurisdiction and a less-documented one is inherently lopsided, and I felt that imbalance directly. India's regulatory history on this subject is extensively litigated, debated, and written about in English-language sources, with a clear timeline running from the RBI's original circular through the Personal Data Protection Bill's various iterations to the DPDP Act. Uzbekistan's framework, by contrast, is still consolidating, and much of the useful material exists only in Uzbek or Russian, or in early-stage regulatory guidance rather than settled jurisprudence. I leaned on TSUL coursework and faculty guidance, including the supervision of Dr. Islombek Abdikhakimov, and I remain conscious that this is the methodologically weaker leg of the comparison. I have tried to be honest about that limitation in the dissertation itself rather than overstating symmetry between the two systems.

I also wrestled with scope throughout. Data localization touches competition law, national security law, consumer protection, and technical infrastructure policy all at once, and every additional angle I opened threatened to turn a focused dissertation into an unfocused survey. Narrowing deliberately to payment service providers, rather than data localization in general, was the single decision that made the project manageable, and in hindsight I wish I had made it earlier instead of drafting extra chapters I later cut.

Cross-Border Friction as the Real Compliance Burden

If there is one theme that recurs throughout the material, it is that the hardest compliance problems do not arise within either jurisdiction in isolation, they arise at the seams between jurisdictions. A payment service provider operating in both India and Uzbekistan cannot satisfy each country's localization mandate independently, because neither mandate was designed with the other in mind. Cloud providers must build genuinely separate, geo-isolated infrastructure in each country rather than a single shared regional deployment, which raises both capital cost and operational complexity, particularly where hyperscale providers lack a uniform localized footprint and PSPs must rely on local, state-approved data-centre partners instead. Data portability rights under both statutes create a further tension, since honoring an individual's right to move their data can directly conflict with a mandate restricting where that data may travel. SWIFT messaging for cross-border remittances compounds the problem further, since it inherently spans multiple jurisdictions in a way strict localization regimes were never built to accommodate cleanly.

This is where the strategic recommendations underlying the dissertation earn their place, particularly the case for jurisdiction-specific data architectures and bilateral data-governance arrangements between India and Uzbekistan. Neither country is likely to relax its localization stance, since the political and economic logic behind both regimes is too well established, so the realistic path forward is not deregulation but interoperability: harmonized cybersecurity certification, mutual-recognition frameworks, joint regulatory sandboxes, and structured regulatory dialogue that reduces duplicated audit burden without diluting either country's sovereign control over its data.

How This Connects to My Practice

Because my consulting work involves market entry and in-country representation for foreign firms, this dissertation is not purely academic for me. The comparative framework I have built, particularly the way it separates storage mandates from cross-border transfer conditions, is something I expect to draw on directly when advising clients as they begin using digital payment rails across these markets. Understanding the RBI's approach in operational detail, and being able to explain to a foreign client why India's regime is stricter in practice than Uzbekistan's current framework, has already sharpened conversations I have had this year.

Looking Ahead

If I were to extend this work beyond the dissertation, I would want to track how Uzbekistan's framework matures over the next two to three years, since it is clearly still being written in real time, and whether India's DPDP Act rules, once fully notified, tighten or relax the existing RBI position for payment data specifically. For now, this dissertation has done what I hoped it would: it has forced a genuinely comparative, evidence-based understanding of two regulatory paths that, at first glance, looked like variations on the same theme, and turned out on closer study to be shaped by very different institutional histories and very different stages of digital financial market development.

Bibliography

1. Information Technology Act, 2000, No. 21 of 2000 (India), s. 43A.
2. Reserve Bank of India, Circular on Storage of Payment System Data, RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018 (6 April 2018).
3. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
4. Indian Computer Emergency Response Team (CERT-In), Directions relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents, No. 20(3)/2022-CERT-In (28 April 2022).
5. Law of the Republic of Uzbekistan "On Personal Data", No. ZRU-547 (2 July 2019).
6. Presidential Decree of the Republic of Uzbekistan on the "Digital Uzbekistan 2030" Strategy, UP-6079 (2020).
7. Law of the Republic of Uzbekistan "On Electronic Commerce" (2020, as amended).
8. Central Bank of the Republic of Uzbekistan, Regulation on Payment Systems (2021).
9. Law of the Republic of Uzbekistan "On Cybersecurity" (2023).
10. Code of Administrative Responsibility of the Republic of Uzbekistan (as amended, provisions on data protection and payment system violations).
11. National Payments Corporation of India, Unified Payments Interface (UPI) – Procedural Guidelines and Product Overview, npci.org.in.
12. Uzcard Company and Humo Payment System, Central Bank of Uzbekistan Interbank Settlement System (UZIPS) – Operational Overview.
13. United Nations Conference on Trade and Development (UNCTAD), Data Protection and Privacy Legislation Worldwide, unctad.org.
14. European Commission, Adequacy Decisions under the General Data Protection Regulation, ec.europa.eu.
15. SWIFT, Cross-Border Payments and Messaging Standards Overview, swift.com.
16. Reserve Bank of India, Master Directions on Prepaid Payment Instruments and Payment Aggregators (as amended).
17. Central Bank of the Republic of Uzbekistan, Annual Report on Digital Financial Inclusion and Islamic Finance Developments.