INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE EVOLUTION OF FINTECH REGULATION IN INDIA: FROM PAYMENT SYSTEMS TO DIGITAL FINANCIAL GOVERNANCE

AUTHOR – PRAVIN RAJ, LLM - CYBER SPACE LAW AND JUSTICE DEPARTMENT, SCHOOL OF EXCELLENCE IN LAW, TAMILNADU AMBEDKAR LAW UNIVERSITY CHENNAI PERUNGUDI CAMPUS

BEST CITATION – PRAVIN RAJ, THE EVOLUTION OF FINTECH REGULATION IN INDIA: FROM PAYMENT SYSTEMS TO DIGITAL FINANCIAL GOVERNANCE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (9) OF 2026, PG. 654-667, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

Financial Technology (FinTech) has transformed the structure and delivery of financial services in India by integrating digital innovation with banking, payments, lending, insurance, and investment systems. The rapid expansion of digital payment platforms, Unified Payments Interface (UPI), prepaid payment instruments, neobanks, peer-to-peer lending platforms, digital lending applications, and **algorithm-driven financial services has significantly altered the traditional financial ecosystem**. This technological transition has simultaneously created new opportunities for financial inclusion, economic growth, and digital governance while also **raising serious concerns** relating to consumer protection, cybersecurity, data privacy, money laundering, regulatory arbitrage, and systemic financial risks.

This paper examines the evolution of FinTech regulation in India from a payment-system-centric model to a broader framework of digital financial governance. It analyses the regulatory role of institutions such as the Reserve Bank of India, Securities and Exchange Board of India, and Insurance Regulatory and Development Authority of India in shaping India's FinTech ecosystem. The study traces the legislative and policy developments beginning with the Payment and Settlement Systems Act, 2007 and further evaluates subsequent regulatory frameworks governing payment aggregators, prepaid payment instruments, digital lending, peer-to-peer platforms, payment banks, and cybersecurity obligations within financial institutions. The paper also discusses the growing relevance of the Digital Personal Data Protection Act, 2023 and the Information Technology regulatory framework in addressing data governance and digital consent in financial transactions.

The research adopts a doctrinal and analytical methodology by examining statutes, RBI master directions, circulars, committee reports, judicial developments, and policy documents relating to FinTech regulation in India. It further evaluates how the Indian regulatory model attempts to balance technological innovation with financial stability and consumer welfare. Special attention is given to emerging regulatory concerns involving artificial intelligence-based credit scoring, embedded finance, digital frauds, cross-border financial data flows, and the increasing role of regulatory sandboxes in promoting responsible innovation.

The paper argues that although India has emerged as one of the world's leading FinTech markets through initiatives such as Digital India and UPI-led payment infrastructure, the **regulatory ecosystem remains fragmented due to overlapping jurisdictional powers and rapidly evolving technological risks**. It concludes that India requires a more harmonized and adaptive regulatory architecture capable of integrating financial regulation, cybersecurity governance, and data protection standards into a unified digital financial governance framework. The study proposes stronger inter-regulatory coordination, enhanced consumer-centric safeguards, AI accountability mechanisms, and

comprehensive digital risk management policies to ensure sustainable and secure FinTech growth in India.

Aims of the Study and Objectives

To critically examine the evolution of FinTech regulation in India and analyse how the legal framework has transformed from a payment-system-based regulatory model to a broader system of digital financial governance balancing innovation, financial stability, cybersecurity, and consumer protection.

Objectives of the Study

To examine the growth and development of FinTech in India and analyse the evolution of the regulatory framework governing digital payments, payment aggregators, digital lending platforms, prepaid payment instruments, and other FinTech services.

To analyse the role of regulatory authorities such as the Reserve Bank of India, Securities and Exchange Board of India, and Insurance Regulatory and Development Authority of India in regulating and supervising the FinTech ecosystem.

1. To examine the legal and regulatory challenges relating to consumer protection, cybersecurity, digital fraud, financial stability, and data privacy in the FinTech sector, particularly under the Digital Personal Data Protection Act, 2023 and related information technology laws.
2. To analyse emerging issues in digital financial governance, including artificial intelligence-based financial services, algorithmic lending, embedded finance, regulatory sandboxes, and cross-border data governance.
3. To evaluate the effectiveness of the existing FinTech regulatory regime in India and propose recommendations for a more harmonized, adaptive, and consumer-centric digital financial governance framework.

Introduction

Financial Technology (FinTech) has emerged as one of the most transformative developments in the modern financial sector by integrating technology with banking, payments, lending, insurance, and investment services. The rapid advancement of digital technologies such as artificial intelligence, blockchain, cloud computing, mobile applications, and digital payment systems has significantly changed the manner in which financial services are accessed and delivered. FinTech has enhanced financial inclusion, improved efficiency, reduced transaction costs, and increased accessibility to financial services for individuals and businesses across the world.

India has become one of the fastest-growing fintech ecosystems globally due to strong digital infrastructure, increasing internet penetration, smartphone usage, and government initiatives such as Digital India, Aadhaar, Jan Dhan Yojana, and the Unified Payments Interface (UPI). The rise of digital wallets, payment aggregators, online lending platforms, insurtech services, and embedded finance has transformed India's financial landscape and accelerated the shift towards a cashless economy. India's high fintech adoption rate reflects the growing reliance on digital financial services among consumers and businesses alike.

Despite its rapid growth and benefits, the expansion of fintech has raised several legal and regulatory concerns relating to consumer protection, cybersecurity, digital fraud, financial stability, and data privacy. India currently follows an activity-based regulatory framework where multiple regulators, including the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), and Insurance Regulatory and Development Authority of India (IRDAI), regulate different fintech activities. In this context, the present study examines the evolution of fintech in India, analyses the existing regulatory framework governing fintech services, and evaluates the challenges and future directions for developing a more harmonized, adaptive, and consumer-centric regulatory regime.

The regulation and supervision of the FinTech ecosystem in India are primarily carried out by the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and the Insurance Regulatory and Development Authority of India (IRDAI), each functioning within its respective financial domain. The RBI acts as the principal regulator for digital payments, payment systems, digital lending, prepaid payment instruments, NBFCs, and banking-related fintech activities by issuing guidelines, licensing fintech entities, and ensuring financial stability and consumer protection. SEBI regulates fintech activities related to securities markets, online trading platforms, robo-advisory services, investment technology, crowdfunding, and algorithmic trading, while also framing cybersecurity and disclosure standards for market intermediaries. IRDAI supervises insurtech platforms and digital insurance services by regulating online insurance distribution, digital policies, and technology-driven insurance practices. Together, these regulatory authorities play a crucial role in promoting innovation, ensuring compliance, protecting consumers, managing technological risks, and maintaining trust and stability within India's rapidly evolving fintech ecosystem.

1. Analysing the role of regulatory authorities such as the Reserve Bank of India, Securities and Exchange Board of India, and Insurance Regulatory and Development Authority of India in regulating and supervising the FinTech ecosystem.

India does not have a single fintech regulator; instead, responsibility is divided among specialized authorities based on the specific financial service provided. The Securities and Exchange Board of India (SEBI) and the Insurance Regulatory and Development Authority of India (IRDAI) regulate distinct fintech sub-sectors to ensure market integrity and consumer protection:

RBI's Regulatory Approach to Fintech

The Reserve Bank of India (RBI) plays a central role in shaping the regulatory environment for fintech in India. Its approach focuses on promoting innovation in digital financial services while ensuring stability, security, and consumer protection. Through structured guidelines and evolving frameworks, the RBI regulates digital payments, lending platforms, and emerging technologies such as open banking and digital currencies.

1. Digital Payments and UPI

The RBI has been a key driver of India's digital payment ecosystem, especially through the Unified Payments Interface (UPI), which has revolutionized real-time fund transfers. The Payment and Settlement Systems Act, 2007 provides the legal foundation for regulating electronic payment systems and ensuring their safety and efficiency. In addition, RBI guidelines for payment aggregators, wallets, and gateways require service providers to maintain strict compliance standards to protect users. The introduction of offline digital payment frameworks further supports financial inclusion by enabling transactions in areas with limited internet connectivity

2. Digital Lending Regulations

The rapid expansion of digital lending platforms has raised concerns regarding predatory lending practices, transparency, and misuse of customer data. In response, the RBI issued the Digital Lending Guidelines in 2022 to regulate such platforms. These rules require full disclosure of loan terms, identification of regulated lending entities, and prohibition of unauthorised intermediaries. The RBI also emphasizes strong data protection norms to safeguard borrower information and prevent exploitation.

3. RegTech and Open Banking

To improve efficiency and transparency in financial services, the RBI has introduced regulatory technology (RegTech) initiatives such as the Account Aggregator framework. This system enables secure and consent-based sharing of financial data between institutions, forming the basis of open banking in India. Alongside this, strict Know Your Customer (KYC) norms and digital onboarding procedures are enforced to reduce fraud, strengthen identity verification, and enhance the integrity of financial transactions.

RBI's Stance on Cryptocurrency

The RBI has maintained a cautious stance on cryptocurrencies due to concerns over financial stability, consumer protection, and illicit financial activities. It argues that unregulated crypto assets may disrupt monetary policy and increase risks of fraud and money laundering. In 2018, RBI restricted banks from dealing with crypto-related businesses, but this restriction was overturned by the Supreme Court in 2020, allowing crypto trading to continue. Meanwhile, the government has explored regulatory options, including the possibility of a dedicated crypto framework and the introduction of a Central Bank Digital Currency (CBDC), known as the digital rupee.

1. RBI's Concerns About Cryptocurrencies

The RBI views cryptocurrencies as a potential threat to financial stability due to their volatile and unregulated nature. Concerns include risks of money laundering, fraud, and lack of investor protection. The anonymity of crypto transactions further complicates regulatory oversight, making them vulnerable to misuse for illegal activities.

2. RBI Ban and Supreme Court Reversal

In 2018, the RBI issued a circular restricting banks from providing services to cryptocurrency businesses, effectively limiting their operation in India. However, in 2020, the Supreme Court struck down this restriction, stating it was disproportionate, thereby restoring access to banking services for crypto exchanges and users.

3. Regulatory Framework for Crypto in India

India continues to explore a formal regulatory structure for cryptocurrencies through proposed legislation such as the Cryptocurrency and Regulation of Official Digital Currency framework. At the same time, the RBI is actively developing the Central Bank Digital Currency (CBDC), which aims to provide a government-backed digital alternative to private cryptocurrencies while maintaining monetary control.

Challenges in Regulating Fintech and Cryptocurrency

Regulating fintech and crypto presents multiple challenges. A major issue is balancing innovation with regulation—too much control may hinder technological growth, while too little may increase risks. Data security and privacy are also critical concerns due to rising digital transactions. Additionally, cross-border regulatory coordination remains complex, especially for decentralized crypto assets. Preventing financial crimes such as money laundering and fraud is another ongoing challenge.

Future Outlook

The future of fintech regulation in India is expected to involve tighter regulatory frameworks, particularly in digital lending, payments, and data governance. The RBI is likely to strengthen compliance systems while supporting innovation. The rollout of the Central Bank Digital Currency (CBDC) represents a major shift toward sovereign digital money. In the case of cryptocurrencies, India may move toward a regulated framework rather than a complete ban, aiming to balance innovation with investor protection.

Securities and Exchange Board of India, and Insurance Regulatory and Development Authority of India –

Role of SEBI and IRDAI in Regulating FinTech Laws in India

Alongside the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI) and the Insurance Regulatory and Development Authority of India (IRDAI) play a crucial role in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 9 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

regulating India's evolving fintech ecosystem. Their regulatory focus extends to capital markets, investment platforms, insurance technology (InsurTech), and digital financial advisory services, ensuring that innovation does not compromise investor and consumer protection.

Securities and Exchange Board of India (SEBI)

SEBI regulates fintech activities that intersect with capital markets and investment services. With the rise of digital trading apps, robo-advisors, algorithmic trading platforms, and online investment platforms, SEBI has strengthened its regulatory oversight to ensure transparency, market integrity, and investor protection. Fintech companies offering services such as stock trading, mutual fund distribution, and portfolio management must comply with SEBI regulations governing intermediaries, disclosure norms, and investor grievance mechanisms. SEBI also monitors risks related to algorithmic trading and unregulated financial influencers on digital platforms, ensuring that investors are not misled by misleading financial advice or unregistered entities. Through its regulatory sandbox framework, SEBI also supports innovation by allowing fintech firms to test new products under controlled conditions.

Insurance Regulatory and Development Authority of India (IRDAI)

IRDAI regulates the InsurTech segment of fintech, which includes digital insurance platforms, online policy aggregators, and automated insurance underwriting systems. With increasing digitisation of insurance services, IRDAI ensures that policyholders are protected from mis-selling, data misuse, and unfair practices. Insurance aggregators and web-based insurance distributors are required to follow strict licensing norms and transparency requirements. IRDAI also promotes innovation through initiatives like the regulatory sandbox, allowing insurance startups to experiment with new digital models such as AI-based claims processing and usage-based insurance products. At the same time, it maintains strong consumer protection standards to ensure that digital insurance services remain fair, accessible, and reliable.

Regulatory Roles in FinTech: RBI vs SEBI vs IRDAI

Regulator	Core Sector	FinTech Areas Covered	What They Specifically Do
RBI (Reserve Bank of India)	Banking & Payments, UPI, wallets, payment	UPI, wallets, payment gateways, digital lending, CBDC (digital rupee), account aggregators	Regulates digital payments infrastructure, issues guidelines for payment systems, controls digital lending norms, supervises NBFC-based fintech lending, and manages monetary stability in digital finance **Key Focus**: Payment security, financial stability, consumer protection, credit regulation
SEBI (Securities and Exchange Board of India)	Capital Markets & Investments	Stock trading apps, robo-advisors, mutual fund platforms, algorithmic trading systems, investment advisory fintech	Regulates digital payments infrastructure, issues guidelines for payment systems, controls digital lending norms, supervises NBFC-based fintech lending, and manages monetary stability in digital finance **Key Focus** Investor protection, market transparency, capital market integrity

IRDAI (Insurance Regulatory and Development Authority of India)	Insurance Sector	InsurTech platforms, online insurance aggregators, digital underwriting, AI-based claims processing	Regulates digital insurance distribution, licensing of insurance intermediaries, policyholder protection, grievance redressal, and approval of insurance tech innovations through sandbox **Key Focus**: Consumer protection, insurance transparency, risk management

2. examining the legal and regulatory challenges relating to consumer protection, cybersecurity, digital fraud, financial stability, and data privacy in the FinTech sector, particularly under the Digital Personal Data Protection Act, 2023 and related information technology laws.

I. The Structural Problem: Multi-Regulator Fragmentation

India's FinTech sector is uniquely exposed to regulatory confusion because no single authority has comprehensive oversight. The RBI governs payments and lending, SEBI covers investment platforms, IRDAI oversees InsurTech, and MeitY administers digital infrastructure laws — but none of these mandates were designed with technology-first financial companies in mind. The result is regulatory arbitrage: companies deliberately structure themselves to fall under the lightest regulatory touch.

II. Digital Personal Data Protection Act, 2023 — Core FinTech Conflicts

The DPDPA is the most significant legislative development for FinTech in a generation. Its key tensions with existing financial law are:

Consent vs. Legitimate Use: The DPDPA requires free, specific, and unconditional consent. However, many FinTech functions — fraud detection, AML monitoring, credit risk assessment — depend on processing data without granular consent. The law creates "certain legitimate uses" exceptions, but these are narrowly defined and untested.

Storage Limitation vs. PMLA Retention: The DPDPA mandates deletion of data once the purpose is fulfilled. PMLA requires KYC and transaction records to be retained for five to ten years. No reconciliation mechanism exists in either statute, leaving FinTechs in structural non-compliance whichever rule they follow.

Account Aggregator Conflict: RBI's Account Aggregator (AA) framework, which enables consent-based financial data sharing, was designed before the DPDPA. The AA's "consent artefact" mechanism and the DPDPA's consent rules operate on different standards, creating implementation uncertainty for the entire Open Banking ecosystem.

III. Cybersecurity — Laws Lagging Technology

The IT Act 2000 (as amended in 2008) was drafted before smartphones, UPI, and AI-enabled fraud existed. Its most critical gaps for FinTech are:

- **No sector-specific cybersecurity standard** — the Sensitive Personal Data Rules 2011 are technology-agnostic; RBI's 2023 Master Direction on IT applies only to banks and NBFCs, leaving Payment Aggregators, LSPs, and WealthTech platforms in a grey zone.
- **CERT-In's 6-hour reporting window** (introduced 2022) is operationally demanding for smaller FinTechs without 24/7 security operations centres.
- **Deepfake and AI fraud** — crimes enabled by synthetic identities or AI-generated

voice/video fall under existing fraud provisions (IPC Section 420, IT Act Section 66D), but prosecution requires proving mens rea (criminal intent) in systems that operate autonomously — a near-impossible evidentiary standard.

IV. Consumer Protection — Rights Without Effective Remedies

The Consumer Protection Act 2019 is broad enough to cover most FinTech wrongs — dark patterns, hidden fees, misleading robo-advisory — but enforcement is undermined by:

Forum multiplicity: A consumer defrauded by a digital lender could theoretically approach the RBI Ombudsman, the Consumer District Forum, the Data Protection Board (if data was misused), and SEBI (if investment products were involved). There is no single-window redressal mechanism.

Platform liability ambiguity: When a Lending Service Provider (LSP) acting through an app commits a violation, RBI's 2022 Digital Lending Guidelines hold the Regulated Entity (bank/NBFC) liable — but the consumer typically has no direct contractual or statutory claim against the LSP itself, making recovery difficult.

Algorithm opacity: No Indian statute currently requires a FinTech to explain to a customer why their loan was rejected or their risk profile was downgraded by an AI model. The EU's GDPR provides a "right to explanation" for automated decisions — India has no equivalent.

V. Financial Stability — Systemic Risks

Concentration in payments: India's UPI ecosystem processes over 100 billion transactions annually, with three apps accounting for the overwhelming majority of volume. A cyberattack or operational failure at any one of these entities could trigger systemic disruption — yet there is no formal "critical infrastructure" designation with special obligations.

BNPL and credit risk: Buy Now Pay Later products operate at the intersection of payment services and lending regulation. Many early BNPL providers structured themselves to avoid NBFC registration, operating without capital adequacy norms, exposure limits, or fair practices codes until the RBI's 2022 Digital Lending Guidelines closed most gaps.

Crypto regulatory vacuum: Despite PMLA coverage for AML purposes, India has no investor protection framework for Virtual Digital Asset (VDA) exchanges. When an exchange fails or is hacked, retail investors have no statutory recourse equivalent to deposit insurance or securities investor protection.

VI. Priority Recommendations

The interactive widget above details eight specific reforms. The three most urgent are:

1. **Reconcile DPDPA with PMLA** through a Joint Ministerial Order providing sector-specific carve-outs with appropriate safeguards — without this, every regulated FinTech is in technical non-compliance with one statute or the other.
2. **Mandate algorithm explainability** for credit and investment decisions through RBI and SEBI regulations, giving consumers a meaningful right to challenge automated adverse decisions.
3. **Establish a unified FinTech grievance portal** that routes complaints to the correct regulator automatically — the current multi-forum system effectively denies justice to consumers who cannot navigate jurisdictional boundaries.

The interactive panel above allows you to explore each domain — DPDPA obligations, cybersecurity framework, consumer protection, financial stability risks, and reform recommendations — in detail. Each section draws on the relevant statutory provisions and regulatory instruments.

Analyse emerging issues in digital financial governance, including artificial intelligence-based financial services, algorithmic lending, embedded finance, regulatory sandboxes, and cross-border data governance

I. AI-Based Financial Services — Governing the Ungovernable?

The central governance challenge with AI in financial services is what regulators call the "black box problem": AI systems produce outcomes — loan approvals, fraud flags, investment recommendations — without generating the kind of decision trail that traditional regulatory oversight depends on. India's existing frameworks were built for human-supervised, rule-based financial decision-making and are structurally inadequate for autonomous AI.

The most urgent gap is the absence of a right to explanation for adverse AI-based financial decisions. When an AI system rejects a loan application or flags a transaction as fraudulent, no Indian statute — not the DPDPA, not the Consumer Protection Act, not any RBI circular — gives the affected individual a right to an intelligible explanation. This stands in stark contrast to the EU AI Act 2024, which classifies credit scoring as a "high-risk AI system" and mandates human oversight, transparency, and redress. India's MeitY has issued non-binding AI advisory guidelines, but these have no regulatory force and no sector-specific application to financial services.

Generative AI introduces a second wave of risk that existing frameworks are wholly unequipped to address. Large language models being deployed in banking chatbots and financial advisory applications can "hallucinate" — generating plausible but factually incorrect financial information. When this misinformation causes consumer loss, no liability chain in Indian law cleanly attributes responsibility between the AI developer, the financial institution deploying it, and the consumer.

II. Algorithmic Lending — Speed Without Safeguards

Algorithmic lending has extended credit to segments of the Indian population that formal banking never reached — an achievement of genuine developmental significance. The governance challenge is that this expansion has been accomplished largely without the procedural protections that accompanied traditional lending: credit bureau verification, human underwriting review, documented credit assessment rationale.

The Account Aggregator (AA) framework represents India's most ambitious attempt to create a consent-based data infrastructure for algorithmic lending. By allowing consumers to share their financial data with lenders through a regulated intermediary, it aims to enable cash-flow-based credit assessment without requiring borrowers to photocopy bank statements. The practical tension is between the AA's consent model — which bundles multiple purposes into a single consent artefact — and the DPDPA's requirement for consent that is specific and unconditional. These two frameworks were designed by different arms of government without coordination, and the incompatibility has never been formally resolved.

The First Loan Default Guarantee (FLDG) mechanism deserves particular attention as a systemic risk concern. Under FLDG arrangements, LSPs provide de facto credit guarantees to the banks and NBFCs that actually originate the loans. This creates an off-balance-sheet risk transfer that replicates, in the digital lending space, the kinds of structured credit risk that contributed to global financial instability in 2008. RBI's September 2023 circular on FLDG partially addresses this, but the capital implications for LSPs (which are not prudentially regulated) remain unresolved.

III. Embedded Finance — The Perimeter Dissolution

Embedded finance is analytically the most interesting of the five domains because it does not merely raise questions about how to regulate a new financial product — it challenges the foundational architecture of financial regulation itself. That architecture assumes a clear distinction between financial firms (which are licensed and supervised) and non-financial firms (which are not). Embedded finance dissolves this boundary.

When a ride-hailing app offers its drivers a working capital loan, or an e-commerce platform offers checkout credit, or an agritech platform offers input financing — the customer-facing entity is not a financial institution. It holds no RBI licence. It is regulated, if at all, by the Information Technology Act and consumer protection laws designed for general commerce. Yet it is performing the economic function of financial intermediation, with all the attendant risks to consumers and the financial system.

The "pass-through" approach — where the regulated NBFC or insurer sits behind the platform and the platform acts merely as a distributor — is how most embedded finance currently operates in India. This structure creates a crucial liability gap: the regulated entity is responsible for the underlying financial product, but the customer-facing conduct (the interface, the disclosures, the sales process, the dispute handling) is controlled by the unregulated platform. RBI's Lending Service Provider framework partially addresses this for credit products, but embedded insurance, embedded investment, and embedded payments each operate under different and less complete frameworks.

IV. Regulatory Sandboxes — Innovation or Arbitrage?

India now has at least five parallel sandbox frameworks (RBI, SEBI, IRDAI, PFRDA, IFSCA), each with different eligibility criteria, testing parameters, data rules, and exit pathways. This fragmentation is particularly damaging for hybrid products — a credit-linked health insurance product, for example, sits at the intersection of RBI and IRDAI jurisdiction and fits neatly into neither sandbox.

The consumer protection deficit in India's sandbox frameworks is significant. Sandbox participants are partially exempt from standard regulatory requirements — that is precisely what makes the sandbox useful for innovation. But it also means that the consumers who participate in sandbox tests have fewer protections than they would in the regulated market. No Indian sandbox framework maintains a compensation fund for consumer losses during testing. Consent disclosure for sandbox participation is governed only by general consumer protection law, with no specific requirement to explain to test participants that the product they are using has not been fully approved.

The CBDC pilot — India's e-Rupee — represents a particularly consequential sandbox that has received insufficient governance scrutiny. Retail CBDC raises profound questions about financial privacy (the RBI would have access to every retail transaction), programmability (can the government restrict what e-Rupee can be spent on?), and the implications for financial inclusion if the privacy architecture is weak.

V. Cross-Border Data Governance — The Unresolved Infrastructure Problem

India's cross-border data governance challenge has a structural quality that distinguishes it from the other four domains: the problem cannot be solved by India alone. Global payment networks (SWIFT, Visa, Mastercard), global cloud infrastructure (AWS, Azure, GCP), global capital markets, and global AML/CFT frameworks all require cross-border data flows as a technical and legal matter. India's data localisation requirements, however well-intentioned, create operational friction with all of these systems simultaneously.

The most acute unresolved issue is the DPDPA's "notified country" framework for cross-border transfers. The Act came into force in August 2023, but the list of countries to which personal data may be transferred has not yet been published. This creates a legal limbo for every Indian FinTech with any international component — they are technically in breach of a law that has not yet been made operationally meaningful.

GIFT City's IFSCA framework creates a potentially productive escape valve: by routing international FinTech operations through the

International Financial Services Centre, entities can access more liberal data transfer rules. The risk is that this becomes a route for regulatory arbitrage — a "data haven" within India that undermines the domestic framework's goals — rather than a genuine platform for internationally competitive financial services.

The interaction between data governance and AML/CFT obligations deserves particular attention. India's Financial Intelligence Unit (FIU-IND) participates in the Egmont Group of financial intelligence units and is obligated under FATF Recommendations to share suspicious transaction data with foreign FIUs. The DPDPA's exemptions for "national security" and "prevention of offences" may cover this sharing, but the scope is uncertain and has not been tested. This uncertainty creates risk for Indian FinTechs that process cross-border transactions and need to cooperate with foreign regulators on fraud and money laundering investigations.

The risk and readiness matrix in the final tab of the interactive panel above summarises India's position across all five domains, with urgency ratings and global benchmark comparisons. The six priority recommendations identify the minimum legislative and regulatory interventions needed to bring India's digital financial governance framework to a level commensurate with the scale and sophistication of its FinTech sector.

To evaluate the effectiveness of the existing FinTech regulatory regime in India and propose recommendations for a more harmonized, adaptive, and consumer-centric digital financial governance framework.

Evaluation of the Existing FinTech Regulatory Regime in India and Recommendations for a Harmonized Digital Financial Governance Framework

India's FinTech ecosystem has emerged as one of the fastest-growing digital financial markets globally, supported by strong digital infrastructure, expanding internet penetration, and government initiatives promoting financial inclusion. Regulatory institutions such as the Reserve Bank of India, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India, and the Ministry of Electronics and Information Technology have introduced various laws, regulations, and guidelines to supervise digital payments, lending platforms, payment aggregators, insurance technology, crowdfunding, and data governance. While the existing regulatory regime has significantly contributed to innovation and financial inclusion, several structural and operational challenges continue to affect the effectiveness of digital financial governance in India.

Effectiveness of the Existing FinTech Regulatory Framework

The Indian FinTech regulatory framework has achieved considerable success in promoting digital transactions, enhancing financial access, and strengthening payment infrastructure. Initiatives such as the Unified Payments Interface (UPI), Aadhaar-enabled verification systems, digital KYC mechanisms, and regulatory sandboxes have accelerated digital financial participation across urban and rural sectors.

Key strengths of the present framework include:

- Promotion of cashless and digital financial systems.
- Increased financial inclusion through simplified digital banking services.
- Strong regulatory supervision of payment systems and digital lending platforms.
- Introduction of cybersecurity and data protection obligations.
- Encouragement of innovation through sandbox frameworks.

The Reserve Bank of India has played a central role in regulating payment systems, prepaid payment instruments, digital lending, and payment aggregators under the Payment and Settlement Systems Act, 2007. Similarly, the Securities and Exchange Board of India regulates

FinTech activities connected with securities markets, robo-advisory services, crowdfunding, and digital investment platforms, while the Insurance Regulatory and Development Authority of India supervises InsurTech innovations.

Despite these advancements, the existing regulatory regime faces several limitations.

Challenges and Regulatory Gaps

Fragmented Regulatory Structure

India's FinTech regulation remains divided among multiple sectoral regulators. Banking, securities, insurance, data governance, and digital commerce are supervised independently, often leading to overlapping jurisdiction and regulatory uncertainty. Many FinTech companies operate across sectors, making fragmented regulation ineffective for integrated digital financial ecosystems.

Inadequate Consumer Protection

Digital financial consumers continue to face risks relating to:

- Unauthorized digital lending,
- Hidden charges and unfair contract terms,
- Misuse of personal data,
- Cyber fraud and phishing attacks,
- Algorithmic discrimination in digital credit systems.

Existing grievance redressal mechanisms are often slow and inaccessible for ordinary consumers, particularly in rural areas.

Data Privacy and Cybersecurity Concerns

Although the Parliament of India enacted the Digital Personal Data Protection Act, 2023, concerns remain regarding:

- Cross-border data transfers,
- Consent-based data processing,
- Data localization,
- Third-party data sharing,
- Cyber resilience of FinTech platforms.

The rapid growth of artificial intelligence and algorithmic financial services has further intensified concerns regarding surveillance, profiling, and automated decision-making.

Regulatory Lag Behind Innovation

Technological innovation in areas such as embedded finance, decentralized finance, crypto-assets, AI-based financial advisory systems, and digital assets evolves faster than regulatory responses. Existing laws were primarily designed for traditional banking and financial institutions and may not adequately address emerging digital financial models.

Compliance Burden on Startups

Smaller FinTech startups often face high compliance costs due to multiple licensing requirements, sectoral approvals, and reporting obligations. Excessive compliance burdens may discourage innovation and market entry.

Recommendations for a Harmonized and Adaptive Framework

To improve the effectiveness of digital financial governance, India requires a more coordinated, technology-sensitive, and consumer-oriented regulatory approach.

Establishment of a Unified FinTech Coordination Mechanism

A centralized inter-regulatory FinTech coordination body should be established involving the Reserve Bank of India, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India, and data protection authorities. Such coordination would:

- Reduce regulatory overlap,
- Improve policy consistency,
- Facilitate integrated supervision of hybrid financial products,
- Promote regulatory harmonization.

Strengthening Consumer-Centric Governance

Consumer protection should become the central objective of FinTech governance. Regulators should:

- Introduce simplified disclosure standards,
- Ensure transparent digital lending practices,
- Mandate explainability for AI-driven financial decisions,
- Strengthen grievance redressal systems,
- Expand digital financial literacy programs.

Special protection mechanisms should also be developed for vulnerable consumers and first-time digital users.

Development of AI and Algorithmic Accountability Standards

India should introduce sector-specific guidelines governing artificial intelligence in financial services. These standards should address:

- Algorithmic transparency,
- Bias testing,
- Human oversight,
- Auditability of automated systems,
- Accountability for AI-generated decisions.

Such measures would improve trust and fairness within digital financial systems.

Adoption of Principle-Based and Technology-Neutral Regulation

Instead of regulating specific technologies, regulators should adopt activity-based and risk-based regulatory models focusing on:

- Nature of financial activity,
- Level of consumer risk,
- Systemic importance,
- Operational resilience.

This approach would allow regulatory flexibility while accommodating future technological innovation.

Enhancing Cybersecurity and Data Governance

FinTech entities should be required to maintain stronger cybersecurity standards, periodic security audits, breach disclosure obligations, and secure data-sharing practices. Coordination between financial regulators and cybersecurity agencies should be strengthened to address increasing digital fraud and cyber threats.

Expansion of Regulatory Sandboxes

Regulatory sandbox frameworks should be made more inclusive and collaborative by:

- Allowing cross-sector participation,
- Simplifying eligibility conditions,
- Supporting startup experimentation,
- Encouraging responsible innovation under supervisory oversight.

A unified national sandbox framework may improve consistency across regulatory sectors.

Conclusion

The Indian FinTech regulatory regime has made substantial progress in promoting innovation, financial inclusion, and digital payment infrastructure. However, the increasing complexity of digital financial ecosystems requires more coordinated, adaptive, and consumer-centric governance mechanisms. Fragmented regulation, cybersecurity risks, data privacy concerns, algorithmic decision-making, and emerging digital business models present significant governance challenges that existing laws cannot fully address.

A harmonized regulatory framework built on inter-regulatory cooperation, technology-neutral principles, strong consumer protection, AI accountability, and adaptive supervision is essential for ensuring sustainable and secure growth of the digital financial sector. By modernizing its regulatory approach, India can strengthen public trust, promote responsible innovation, and position itself as a global leader in digital financial governance.

Primary Statutes and Legislative References

1. Reserve Bank of India, *Payment and Settlement Systems Act, 2007*
Governs payment systems, UPI regulation, payment aggregators, and digital payment infrastructure in India.
Payment and Settlement Systems Act, 2007

2. Parliament of India, *Digital Personal Data Protection Act, 2023*
Governs consent, data processing, cross-border transfer, and digital privacy obligations applicable to FinTech platforms.
Digital Personal Data Protection Act, 2023

3. Parliament of India, *Information Technology Act, 2000*
Provides legal framework for electronic records, cyber offences, cybersecurity obligations, and digital transactions.
Information Technology Act, 2000

4. Parliament of India, *Consumer Protection Act, 2019*
Relevant for digital consumer protection, unfair trade practices, misleading digital financial services, and grievance mechanisms.
Consumer Protection Act, 2019

5. Parliament of India, *Prevention of Money Laundering Act, 2002 (PMLA)*
Important for AML/KYC compliance obligations applicable to digital finance and crypto entities.
PMLA Act, 2002

RBI Regulations, Master Directions, and Circulars

Digital Lending

6. Reserve Bank of India, *Guidelines on Digital Lending, 2022*
Core framework governing digital lending apps, Lending Service Providers (LSPs), disclosure obligations, and borrower protection.
RBI Digital Lending Guidelines 2022

7. Reserve Bank of India, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps (2021)*
Foundational policy report behind the RBI digital lending framework.
RBI Working Group Report on Digital Lending

Payment Aggregators and Payment Systems

8. Reserve Bank of India, *Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020*
Governs payment aggregators, merchant onboarding, escrow mechanisms, and compliance obligations.
RBI Payment Aggregator Guidelines

9. National Payments Corporation of India, *Unified Payments Interface (UPI) Framework*
Foundational infrastructure document for India's UPI ecosystem.
NPCI UPI Official Website

10. Reserve Bank of India, *Master Directions on Prepaid Payment Instruments (PPIs), 2021*
Governs wallets, prepaid cards, and digital stored-value instruments.
RBI Master Directions on PPIs

Account Aggregator and Open Banking

11. Reserve Bank of India, *NBFC-Account Aggregator Framework*
Governs consent-based financial data sharing and India's open banking ecosystem.
RBI Account Aggregator Framework

12. Sahamati, *Account Aggregator Ecosystem Documentation*
Important practical source explaining consent artefacts and AA architecture.

Sahamati Account Aggregator Resources

Cybersecurity and IT Governance References

13. Indian Computer Emergency Response Team, *CERT-In Directions, 2022* Introduced mandatory cybersecurity incident reporting within six hours. CERT-In Cybersecurity Directions 2022

14. Reserve Bank of India, *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023* Governs cybersecurity governance in banks and NBFCs. RBI IT Governance Directions 2023

15. Ministry of Electronics and Information Technology, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* Core data protection rules prior to the DPDPA framework. SPDI Rules 2011

SEBI and Capital Market FinTech References

16. Securities and Exchange Board of India, *SEBI Regulatory Sandbox Framework* Governs innovation testing for fintech products in securities markets. SEBI Regulatory Sandbox Framework

17. Securities and Exchange Board of India, *Cyber Security and Cyber Resilience Framework for Stock Brokers and Depository Participants* Relevant for algorithmic trading and investment platforms. SEBI Cybersecurity Framework

IRDAI and InsurTech References

18. Insurance Regulatory and Development Authority of India, *IRDAI Regulatory Sandbox Regulations* Framework for testing InsurTech innovations and digital insurance products. IRDAI Regulatory Sandbox Regulations

19. Insurance Regulatory and Development Authority of India, *Web Aggregator Regulations* Governs online insurance distribution and digital insurance intermediaries. IRDAI Web Aggregator Regulations

Cryptocurrency and CBDC References

20. Internet and Mobile Association of India v. Reserve Bank of India Landmark Supreme Court judgment overturning RBI's banking ban on cryptocurrency businesses. Supreme Court Judgment (IAMAI v RBI)

21. Reserve Bank of India, *Concept Note on Central Bank Digital Currency (CBDC)* Explains India's digital rupee framework and policy rationale. RBI CBDC Concept Note

International and Comparative References

22. European Union, *EU AI Act, 2024* Important comparative source for AI governance and high-risk credit scoring systems. EU AI Act Overview

23. European Union, *General Data Protection Regulation (GDPR)* Comparative source for automated decision-making and "right to explanation." EU GDPR Official Portal

24. Financial Action Task Force, *FATF Recommendations* Important for AML/CFT obligations and crypto compliance discussions. FATF Recommendations

Academic and Research References

25. NITI Aayog – India's Booming FinTech Ecosystem Report

26. World Bank – FinTech and Financial Inclusion in India

27. BIS Papers on FinTech and Financial Stability

28. OECD Digital Finance and FinTech Reports

29. Cambridge Centre for Alternative Finance Research

30. Harvard Kennedy School – AI and Financial Regulation Research