INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 8 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 8 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-7-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

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

VOLUME 5 AND ISSUE 8 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

LEGAL AND REGULATORY APPROACHES TO TECHNOLOGY IN BANKING

AUTHOR - SANJANA AGARWAL, STUDENT AT AMITY LAW SCHOOL, NOIDA, UP

BEST CITATION - SANJANA AGARWAL, LEGAL AND REGULATORY APPROACHES TO TECHNOLOGY IN BANKING, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (8) OF 2025, PG. 864-873, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

The accelerated introduction of technology in the banking industry has transformed financial services, providing improved efficiency, accessibility, and innovation. In India, various digital initiatives like the Unified Payments Interface (UPI), digital lending platforms, artificial intelligence (AI)-based credit scoring, and blockchain technologies have greatly revamped conventional banking. These development processes have, however, created a series of legal and regulatory issues, such as data privacy and protection, cybersecurity risks, algorithmic discrimination, financial fraud, and regulatory arbitrage.

This article critically reviews the legal and regulatory strategies implemented in India to counter these challenges. It discusses major frameworks and guidelines released by the Reserve Bank of India (RBI), the Ministry of Electronics and Information Technology (MeitY), and other concerned authorities. The study highlights the role of instruments such as the RBI's digital lending guidelines, regulatory sandboxes, and IT risk management directives in fostering a balance between innovation and regulation. Furthermore, it considers the gaps in existing laws, such as the absence of a comprehensive data protection regime, and evaluates how India can align its policies with global best practices.

Finally, the article advocates a coordinated, responsive, and future-oriented regulatory approach in order to match technological advances in banking with legal protection and institutional strength.

Introduction

The banking industry stands at a turning point driven by an intricate interlacing of regulatory evolution, financial crises, innovation, and evolving consumer demand. Not only are regulations becoming stricter; they are also getting smarter, with significant focus on transparency, data privacy, and customer protection. A recent Deloitte report highlights the outrageous cost of compliance, which puts banks' compliance costs at over $100 billion annually to meet these demands. This is the reason why banks have to implement innovative technologies so urgently.

Meanwhile, the digitalization era has ushered in a new world where customers demand banking processes to be smooth, secure, and tailored to their needs, compelling banks to innovate at breakneck speeds. This research looks at the technologies driving this transformation - from AI and blockchain to RegTech, and the game-changing realms of DeFi and digital currencies. We'll examine how these technologies are not only essential to cutting through the regulatory fog but also are key drivers in redesigning what banking will be in a digital-first world.[973]

Regulatory Responses and Legal Scholarship

- **Regulatory Technology (RegTech)**

Compliance Automation: RegTech solutions apply AI and machine learning to automate compliance tasks, including AML and KYC transaction monitoring and fulfillment of multiple financial regulations. JPMorgan Chase uses AI to sift through tens of millions of transactions per day, identifying compliance breaches with a high degree of accuracy.

[973] REGULATORY FRAMEWORKS FOR THE INDIAN FINTECH INDUSTRY, March 27, 2023

Standard Chartered Bank uses RegTech to clear KYC in many jurisdictions, reducing processing time and errors by an enormous factor.

Real-Time Reporting: The demand for near-real-time regulatory reporting is growing. ING Bank has put in place RegTech solutions in order to gain immediate insights into transaction monitoring and implement compliance adjustments swiftly. These systems offer automated aggregation, analysis, and reporting of data, minimizing human errors and the risk of regulatory penalties.[974]

Risk Assessment: RegTech also enables risk prediction, using data analytics to anticipate where compliance risks may materialize, in order for banks to take preventive rather than remedial action.

Regulatory Change Management: RegTech products like Compliance.ai use NLP to track and examine regulatory changes, allowing banks to be ahead of compliance requirements in different regions and sectors.

- **Blockchain for Transparency and Compliance**

Immutable Records: Blockchain technology allows for an immutable ledger of transactions, which is crucial for regulatory compliance and audit trails. Santander uses blockchain to enable international payments with transparency and security. RBC explores blockchain for trade finance to reduce fraud and ensure maximum compliance by way of transparent record-keeping.

Smart Contracts: These guarantee compliance by implementing provisions of the contract automatically, hence mandating compliance with regulations like payment verifications on cross-border transactions. Commonwealth Bank of Australia has piloted blockchain smart contracts for compliance on trade, where export controls are mandated automatically.

Regulatory Concerns: While blockchain makes things transparent, it is challenging to maintain privacy as well as data protection legislation compliance. Banks are building hybrid blockchains in which private data is not revealed but transaction integrity is publicly verifiable.

Cross-Border Compliance: Blockchain can facilitate cross-border compliance by having one point of data for all parties, reducing mistakes and enhancing regulation.

- **Artificial Intelligence (AI) and Machine Learning (ML)**

Risk Management: AI and ML are crucial in the detection of fraud, assessing credit risk, and managing market risks through analyzing large data sets for patterns or discrepancies. CitiBank uses AI to identify fraud, reducing false positives significantly. HSBC uses ML for advanced credit assessment, ensuring that it complies with Basel III guidelines for sophisticated risk management.

Customer Due Diligence: AI accelerates and facilitates KYC and AML processes, speeding onboarding while preserving constant compliance using real-time surveillance. Deutsche Bank utilized AI in order to reduce onboarding processes by 50%, while maintaining effectiveness and regulatory compliance.

Compliance and Operational Effectiveness: AI enhances regulatory compliance analytics, aids in decision-making, and automates routine compliance tasks, increasing efficiency and accuracy.

Ethical Implications: With AI playing a greater role, banks are focusing on ethical AI to maintain non-discrimination in applications like loan approval, ensuring fairness as per consumer protection laws.

Challenges: Retaining data integrity and privacy in the use of AI for compliance continues to remain an issue, together with the requirement for AI explainability and transparency of its decision-making process.

- **Data Privacy and Security Technologies**

[974] Sherwood Glazier, Technologies Shaping the Future of Banking

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

VOLUME 5 AND ISSUE 8 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

Privacy-Enhancing Technologies (PETs): Due to GDPR and other similar rules, PETs like differential privacy and homomorphic encryption are indispensable for data processing without sacrificing confidentiality. These tools allow banks to derive insights from data without betraying individual anonymity, finding balance between compliance and business insight.

Cybersecurity Improvements: Pecuniary pressures on information security force banks to invest in upgraded cybersecurity. Barclays uses encryption and penetration tests to comply with information protection standards. "Digital twins" of banking infrastructure emulate cyber attacks in order that security measures can be put in place proactively.

Data Governance: Banks are designing robust data governance frameworks to address data lifecycle in a way that data residency regulations and privacy rules of different areas are complied with.

Zero Trust Security: Moving to a 'never trust, always verify' model, banks like Goldman Sachs implement zero trust architectures, adding layers of security for compliance with data protection regulations.

- **Cloud Computing**

Scalability and Flexibility: Cloud platforms like AWS and Azure provide scalable solutions for compliance testing and reporting. DBS Bank leverages cloud for regulatory reporting of best-in-class. Multi-cloud strategies share workloads, enhancing compliance and resilience.

Cloud Security: Banks use hybrid clouds for control and scalability purposes while ensuring data security. Capital One shows the way cloud can be leveraged for management of secure financial information, setting a compliance standard.

Disaster Recovery and Business Continuity: Cloud computing enhances banks' disaster recovery, critical in the delivery of regulatory compliance during disruptions.

Cloud Regulatory Compliance: Banks must navigate compliance issues like data sovereignty and privacy when they are using cloud facilities, with custom solutions or by aligning with cloud suppliers to ensure that they meet regulations.

- **Digital Identity Management**

Secure Authentication: Stricter digital identity authentication, such as biometric authentication, is necessary for regulatory requirements. BBVA uses facial recognition to onboard customers. Bank of America uses biometrics for secure authentication in its mobile banking application, finding the perfect balance between security and customer experience.

Consent Management: Banks have in place systems of managing customer consent to share data to support open banking compliance. Lloyds Banking Group provides a customer dashboard to control data sharing, compliant with GDPR and PSD2.

Identity Federation: Banks see value in identity federation to enable secure, frictionless interactions between platforms and services to simplify compliance with identity verification requirements across ecosystems.

Privacy and Identity: There needs to be a balance of identity verification versus protection of privacy, and this has brought about the implementation of privacy-by-design approaches in identity management systems.

- **Quantum Computing for Sophisticated Risk Modeling**

Enhanced Risk Simulations: Quantum computing may revolutionize risk modeling to comply with capital adequacy regulations. Quantum computers can carry out calculations faster than traditional computers, allowing for accurate risk estimations.

Encryption Evolution: With the advent of quantum computing, today's encryption methods are at risk. Banks must migrate to quantum-safe cryptography in order to secure

information and comply with data security standards.

Quantum in Compliance: Quantum computing power could transform compliance by computing regulatory information at unprecedented scale and, in the process, automatically pinpoint trends or anomalies that could indicate compliance threats.

Investment and Research: Banks are investing in or collaborating with quantum computing research in order to stay ahead of this technology curve, being compliant in the future.

- **Internet of Things (IoT) in Banking Compliance**

IoT Data for Prevention of Fraud: IoT devices like biometric wearables provide real-time information for fraud prevention. Intelligent ATMs are capable of detecting skimming, enhancing security measures.

IoT Regulatory Challenges: It is hard to manage safe data from IoT devices, prompting banks to formulate strict data governance policies to meet privacy and security regulations.

Customer Experience: IoT has the ability to tailor banking, e.g., intelligent branches adjusting according to customer information, but needs to do so while meeting privacy laws.

IoT and Compliance Monitoring: IoT can monitor compliance in real-time, including monitoring physical movement of cash against reconciliation with accounting records to reduce discrepancies.

- **Cross-Border Banking and Regulations**

Global Standards Harmonization: Banks struggle with compliance amidst different regulatory regimes (e.g., GDPR, CCPA, PSD2). Standardized APIs and blockchain solutions facilitate compliance homogeneity.

Technological Solutions to Harmonization: Blockchain provides one version of truth for auditing, and APIs harmonize data sharing. JPMCoin by JPMorgan Chase is an example of banks' ability to address cross-border payments in a way that is compliant.

Regulatory Cooperation: There is increasing momentum for international regulatory cooperation to harmonize standards, hence easing compliance for internationally operating banks.

Compliance Automation in International Transactions: AI and ML are used to automate compliance checks on international transactions to make them compliant with various jurisdictional requirements.[975]

- **Collaborative Ecosystems for Compliance**

Collaboration with industry: Banks collaborate with FinTechs, regulators, and rivals to innovate around compliance solutions. CitiBank has innovation labs for such cooperation.

Sandbox Environments: Sandboxes allow banks to test compliance technologies in new ways without the risk. Sandbox environments encourage innovation while upholding regulatory standards.

Shared Compliance Platforms: Banks are moving towards shared platforms under which they share common tools and data for reporting regulatory, thus minimizing duplication and increasing accuracy.

Cross-Sector Partnerships: Banks are forming alliances with sectors like insurance or utilities for shared compliance infrastructures, leveraging mutual resources to facilitate regulatory needs.

- **Decentralized Finance (DeFi) and Digital Currencies**

DeFi Impact on Traditional Banking: DeFi offers financial services without the traditional intermediaries, and with this come opportunities and challenges regarding compliance. Banks are examining how they can integrate or affiliate with DeFi platforms to offer regulated environments new services. Example:

[975] Lessons from the rapidly evolving regulation of digital banking, October 1, 2021

JPMorgan Chase with JPM Coin shows how traditional finance can adopt DeFi technologies for regulated environments.

Digital Currencies: Central Bank Digital Currencies (CBDCs) and cryptocurrencies transform finance. CBDCs: Central banks like the Federal Reserve see digital currencies in order to have control of monetary policy and take digital benefits.

Cryptocurrencies: Banks must navigate complex rules on cryptocurrencies, including AML/KYC and consumer protection. Standard Chartered offers crypto custody, answering to this emerging asset class.

Regulatory Challenges: The anonymity of cryptocurrencies necessitates banks to spend on tracking technologies to facilitate financial monitoring and compliance.

Interoperability and Integration: Banks are developing systems to integrate with digital currencies, being compliant while providing these services.

Use Case: Mastercard's collaboration with digital currency firms to enable cryptocurrencies on its network indicates integration under rigorous compliance.

Regulatory Sandbox for Digital Assets: Banks use regulatory sandboxes to test and construct compliant digital asset services in order to ensure they are in accordance with regulatory compliance prior to extensive deployment.

Legal Challenges Arising from Technological Disruption

- **Regulatory Lag and Policy Obsolescence**[976]

Regulatory lag is one of the key challenges of overseeing technology-driven banking. Regulatory lag is a recurring feature that stems from the fact that technological advancement naturally takes place at a pace way above that of the regulatory agencies' response rate. As a result, a majority of today's laws and regulatory policies have no chance in the world before they are overtaken by speed, hence remaining with loopholes in oversight. This delay can be especially problematic when emerging financial products or platforms—like decentralized finance (DeFi), crypto assets, or algorithmic lending—emerge without clearly established legal status. In such cases, financial institutions are able to exploit these gray areas, building unregulated risks that have the potential to destabilize financial systems. Also, the rigidity of most regulatory processes makes it difficult to respond rapidly.

Law-making and rule-making processes take long and involve huge consultations with the stakeholders, limiting the regulators' ability to keep up with the technological shock in real-time. By the time new regulations take effect, technologies underlying them have already changed. For example, early regulations focused on initial coin offerings (ICOs), which have been replaced by newer developments like decentralized autonomous organizations (DAOs) and non-fungible tokens (NFTs). Secondly, regulators may not possess the necessary technical expertise to fully comprehend the consequences of emerging technologies, which would further hinder the process. This distance between innovation and regulation can potentially erode public confidence, stifle good innovation, or—conversely—allow bad practice to get out of hand. To overcome this, regulators must make capacity-building investments, adopt adaptive regulatory models like sandboxes, and become more closely involved with technology developers.

- **Data Privacy and Security Risks**

As financial institutions become increasingly dependent on big data, artificial intelligence, and cloud computing, data privacy and cybersecurity today are a significant challenge for regulators. Although these technologies enable greater efficiency and perspective, they also raise extremely serious questions about the collection, storage, sharing, and guarding of

[976] Apar Gupta, "Data Protection and Banking Technology in India", in S. Deva (ed.), Socio-Legal Aspects of Technology in India (Oxford University Press, 2018)

personal and financial information. Current data protection regimes in many jurisdictions are not robust enough to address the scale and sophistication of modern data ecosystems used in banking. In addition, supervisory oversight is complex where third-party service providers are used by financial institutions or sensitive information is processed in cross-border cloud infrastructure.

This offers a scenario whereby regulatory agencies are unable to require compliance with national privacy laws and yet must deal with global legal controversies, including differences between the EU's GDPR and less demanding data systems in other places. Data privacy violations not only violate consumer rights but may also lead to identity theft, fraud, and loss of trust in the financial system. Regulators are faced with the further task of ascertaining whether the AI-based systems used within banks never even unwittingly propagate bias, discrimination, or intrusiveness with respect to privacy. For instance, if data-biased AI-based algorithms are trained upon data containing biases, then the algorithms would reject credit to targeted demographics perpetually—a condition not easy to discover unless the source code of the algorithm is accessible.

Besides, the higher risk of cyberattacks like ransomware and phishing attacks requires special attention at all times. The regulators will therefore have to apply strict cybersecurity measures while, on the other hand, ensuring banks adhere to privacy standards. Treading the tightrope between innovation and consumer protection is always a delicate matter, and the complexity of data flows in technology-driven banking makes this challenge even more difficult.

- **Challenge of Supervising Decentralized Finance and Cryptocurrencies**

Decentralized finance platforms and cryptocurrencies are two of the most disruptive technologies in modern finance. While these technologies have numerous benefits—democratization of finance, openness, and reduced costs—their inherent Decentralization also poses serious problems for regulation. Traditional systems of regulation are built with centralized actors like banks in mind, which have recognizable management hierarchies, geographic locations, and compliance departments. On the other hand, most DeFi protocols are completely devoid of central control, instead relying on decentralized and self-enforcing smart contracts and governance. Due to such decentralization, it becomes difficult for regulators to force them into compliance, regulate activities, or even determine responsible parties.

Besides, DeFi platforms are generally global in nature, operating across borders with varying regulatory environments for digital assets. For instance, a lending platform developed in one country might have customers globally but not be under the direct jurisdiction of any specific regulator. This renders enforcement challenging and opens the possibility of regulatory arbitrage. The anonymity of most cryptocurrency systems also facilitates illegal applications such as money laundering, terrorist financing, and tax evasion, which become more difficult to track.

In addition, the technical complexity of DeFi protocols can obscure systemic risks. Algorithmic stablecoins or leveraged yield farming strategies, for instance, can be built into unstable financial systems regulators might not even comprehend until a crisis point. This was the case with events such as the collapse of the TerraUSD ecosystem that had international spillovers. To deal with these problems, regulators need to rethink their models of supervision, invest in blockchain forensics, and perhaps implement international standards specifically designed for digital finance. But establishing such frameworks is technically and politically challenging, making DeFi regulation one of the most formidable tasks for financial regulators at present.

- **Technological Disparities and Regulatory Inequality**

While technology enables numerous banking innovations, it can simultaneously exacerbate the differences between institutions and jurisdictions to present a profound regulatory challenge. Large, heavily capitalized banks may spend a considerable amount on best-in-class compliance systems, advanced cybersecurity software, and data analysis solutions, making them competitive winners in regulatory compliance. Small institutions or banks in developing markets may lack the technical and financial capabilities to implement such advanced solutions, leading to disparities in levels of compliance and risk management operations.

This unevenness can cause an unbalanced playing field, in which regulators unwittingly discriminate in favor of bigger players simply because they have a better ability to accommodate technologically sophisticated regulation. It can also cause a form of regulatory exclusion, where smaller institutions view mandated digital systems as too costly or complex and therefore risk being sanctioned or forced out of business. Furthermore, worldwide disparity in digital infrastructure as well as regulatory maturity aggravates the problem. While some countries have completely digital regulatory systems and e-governance models, others remain bogged down with paper-based processes and ancient structures.

This inconsistency does not only complicate the process of establishing global standards but also results in areas of regulatory ignorance where systemic hazards may accumulate unchecked. For stable finance globally, it is therefore essential that the regulators take account of the digital divide and coordinate toward inclusive policymaking. That might involve programs of technical support, capacity development, or phasing of regulations in accordance with various levels of technological preparedness. Without filling these gaps, technology-led regulation runs the danger of exacerbating financial disparities as opposed to eliminating them.

- **Algorithmic Bias and Untransparency in AI Systems**

The use of artificial intelligence (AI) and machine learning in banking has introduced advanced tools for credit scoring, fraud detection, and automated compliance. One of the main issues the regulators now have to deal with is the issue of algorithmic bias and lack of transparency—or so-called "black box" problem. AI systems, particularly deep learning models, operate in a way that is difficult to understand for humans. When such systems make a decision—such as approving or denying a loan, reporting suspicious activity, or setting risk premiums—it is difficult to explain the rationale behind the output. This transparency makes internal audits as well as external regulatory inspections difficult.

Worse, AI systems trained on biased or incomplete data may unwittingly be perpetuating race, gender, geographic, or socio-economic class-based discrimination. For example, if lending records contain discriminatory trends, an AI system may identify and replicate the same, harming targeted communities without the institution's intent. Regulatorily, it is very hard to ensure fairness and accountability in such a system. Such traditional checks of compliance are insufficient since they do not audit AI decision-making.

In addition, there is no standard framework or legal requirement that would compel banks to explain the internal workings of their AI. The explainability is not only aimed at consumers' right to understand why a decision about them was taken but also limits the regulator in acting on malpractice. As artificial intelligence comes increasingly into day-to-day finance, regulators face the challenge of how to compel transparency, equality, and responsibility—particularly where even the originators of the models might be unclear about precisely how decisions get made.

- **Cross-Border Legal Conflicts and Jurisdictional Ambiguity**

As greater numbers of digital banking platforms and fintech services transcend borders, regulators are finding it harder to contend with legal conflicts and issues of jurisdiction. The majority of digital financial products—i.e., cryptocurrencies, neobanks, and cross-border payment apps—are designed to be borderless, serving customers in different countries without having a presence in any single country. This complicates it to determine whose laws apply, who should enforce them, and how the violations of regulation are to be handled.

For example, a website run in one country might have its servers elsewhere, process payments through banks in a third, and host clients from around the world. If Country A's citizen has a fraud issue on this website, and the company neither has any presence nor a presence of law within Country A, it may prove difficult for authorities to investigate or prosecute. This is particularly disturbing in the case of financial crimes such as money laundering, data theft, or models of illegal fundraising because they can exploit these holes in jurisdiction.

The picture is also further complicated by the lack of global harmonized standards. While there are some countries stringently regulating fintech and crypto operations, others provide regulatory havens. This inconsistency offers the perpetrators a chance to benefit from regulatory arbitrage—choosing jurisdictions with the lowest level of regulation. It also puts compliant businesses at a disadvantage. Without harmonized legal regimes, mutual recognition arrangements, and international enforcement arrangements, cross-border digital finance poses a chronic threat to regulatory efficiency. Solving this issue requires increased international cooperation and possibly the formation of supranational regulatory institutions or treaties dedicated solely to regulating digital finance.

- **Overregulation and Innovation Stifling**

As strong as is the argument for regulating sound in tech banking, maybe no less relevant is the threat of overregulation to dissuade technology development and cut back on innovation. In seeking to contain the growing risks, the regulators may end up imposing overly draconian compliance requirements or broad prohibitions which stifle testing and delay innovation adoption of useful technologies. This is particularly common in new markets like blockchain, cryptocurrency, and online lending, where unclear or burdensome rules will drive startups underground, or drive them out of business and into more liberal jurisdictions.

Overregulation also stifles product innovation in traditional banks. As regulatory complexity or uncertainty increases, banks may become risk-averse and unwilling to invest in new technology—even if it has the potential to improve service delivery, reduce costs, or increase financial inclusion. For example, a bank might shy away from integrating AI into its underwriting process if it fears future non-compliance fines due to evolving standards for algorithmic accountability. Similarly, fintech firms may not want to roll out new mobile payment features if they don't know how existing banking laws treat them.

This sobering influence of regulation can suppress competition and render it more entrenched in favor of large incumbents, who possess the economic capacity to navigate complex legal landscapes. Startups and small financial institutions, however, typically cannot afford to match regulatory progress, consult lawyers, or create costly compliance frameworks. Balancing risk minimization and the promotion of innovation is quite possibly the most delicate task regulators must perform. In attempting to navigate around this, several jurisdictions are turning to regulatory sandboxes and flexible supervisory frameworks, but widespread acceptance and convergence of these approaches remain low.

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

VOLUME 5 AND ISSUE 8 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

- **Fragmentation of Digital Identity and KYC Frameworks**

Another critical challenge in the digitalization of banking regulation is the lack of a shared, interoperable platform for digital identity and Know Your Customer (KYC) activities. Identity verification in the digital economy is the foundation for regulatory compliance, enabling anti-money laundering (AML) efforts, anti-fraud tactics, and consumer protection. But identity systems vary significantly from country—and even from bank—to country, creating inefficiencies, additional cost, and variation in compliance.

Most banks still employ manual or semi-electronic KYC processes that are time-consuming, error-prone, and expensive. Where digital identity programs (like India's Aadhaar or Estonia's e-Residency) have been introduced, onboarding and verification are now significantly streamlined. But these systems are rarely interoperable across institutions or borders. Therefore, customers would normally have to go through duplicate identity verification procedures when they interact with several financial platforms or banks, and institutions cannot gather good customer profiles.

From the regulatory point of view, this fragmentation makes tracing illicit financial flows, blacklist enforcement, or sharing of risk intelligence more difficult. Moreover, biometric data privacy concerns, consent management, and cross-platform data sharing add more murkiness to the waters in the regulatory environment. Regulators will have to come up with a way of incentivizing standardized, secure, and privacy-friendly digital identity systems that function across borders. Such efforts will include incentivizing private-public partnerships, taking on decentralized identity technologies (such as blockchain-based ID), and coordinating regulations regarding data retention and sharing. Absent these developments, fragmentation of identity will continue to be at odds with efficiency and integrity in tech-based banking systems.

Conclusion

The intersection of technology and banking in India has huge potential but needs careful legal regulation. Though the Reserve Bank of India and other regulators have brought in some progressive steps like digital lending guidelines, regulatory sandboxes, and IT governance regimes, the rapidity of change in technology needs a more dynamic and responsive model of regulation. Fragmented laws, jurisdictional conflicts, and lack of a single data governance law hamper effective regulation.

India would need to switch to a forward-looking instead of a backward response legal approach from now on. The legal system around data protection, AI morality, cybersecurity, and international online transactions would have to be secured. International coordination, RegTech implementation, and inclusive policymaking with industry participation and civil society can assist in framing a shock-absorbing legal framework. As technology continues to revolutionize banking, the legal and regulatory framework has to catch up so that financial innovation is not achieved at the expense of legal certainty, consumer rights, or systemic stability.

Bibliography

1. Rakesh Mohan, "Technology and Financial Intermediation in India", (2005) 40(49) Economic and Political Weekly 5267.
2. K.C. Chakrabarty, "Information Technology in Banking – A Catalyst to Growth", Speech at the Indian Institute of Banking & Finance (2011), available at https://www.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=627 (last visited May 5, 2025).
3. Reserve Bank of India, Report of the Working Group on FinTech and Digital Banking (2017), available at https://rbidocs.rbi.org.in/rdocs//PublicationReport/Pdfs/WG_FINTCH_DIGITALBANKING.pdf (last visited May 5, 2025).

4. Bimal Patel et al., Banking Law and Negotiable Instruments Act (Eastern Book Company, Lucknow, 2nd edn., 2019).
5. Vinod Kothari, Introduction to Fintech and Legal Challenges in India, (Taxmann Publications, New Delhi, 2020).
6. S. Aparna, "Regulation of Digital Banking in India: An Overview of Challenges and Legal Framework", (2021) 7(1) NLIU Journal of Business Laws 78.
7. Reserve Bank of India, Master Directions – Information Technology Framework for the NBFC Sector (2017), available at https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=10993 (last visited May 5, 2025).
8. Nishith Desai Associates, Fintech in India: A Legal and Regulatory Overview (2021), available at https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/FinTech_in_India.pdf (last visited May 5, 2025).
9. Mehta Prashant, "Legal Challenges of Blockchain and Banking Regulation in India", (2020) 9(2) Indian Journal of Law and Technology 112.
10. Praveen Dalal, "Cyber Law Due Diligence in Indian Banking Sector", (2010) 5(3) Journal of Cyber Law & Policy 45.
11. Financial Stability and Development Council, Sub-Committee Report on FinTech and Digital Lending (2022), available at https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1209 (last visited May 5, 2025).