INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

IJLAR

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

THE NEED FOR FINANCIAL REGULATION IN THE ERA OF FINTECH

AUTHORED BY - MOHANA MEENA H

Abstract

Financial technology, commonly known as FinTech, has transformed the delivery of financial services through digital payments, online lending, mobile banking, algorithmic credit assessment, crowdfunding, robo-advisory services and blockchain-based financial products. These developments have improved the speed, accessibility and convenience of financial transactions while creating new legal and regulatory challenges. The increasing participation of technology companies in financial activities has also blurred the traditional boundaries between financial institutions and technology service providers. Consequently, questions concerning consumer protection, data privacy, cybersecurity, accountability, financial stability and regulatory jurisdiction have become increasingly significant.

This article examines the need for financial regulation in the era of FinTech, with particular reference to the Indian legal and institutional framework. It analyses the role of the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority of India (IRDAI), and other relevant institutions in supervising technology-driven financial activities. It further evaluates the limitations of existing regulatory approaches, including fragmented supervision, regulatory arbitrage, risks arising from third-party service providers, algorithmic discrimination and cross-border financial transactions. The article adopts a doctrinal research methodology based on statutes, regulatory directions, judicial principles and reports published by recognised financial institutions. It argues that financial regulation should not merely restrict technological innovation but should establish a proportionate, transparent and accountable framework that encourages responsible development while protecting consumers and maintaining financial stability. The article concludes that India requires coordinated regulatory supervision, stronger technological safeguards, effective grievance redressal, greater algorithmic transparency and continuous adaptation of financial laws to emerging technological developments.

Keywords: FinTech, financial regulation, Reserve Bank of India, digital lending, consumer protection, cybersecurity, data privacy, financial stability, regulatory technology, India.

Introduction

The financial sector has undergone a substantial transformation due to the integration of technology into banking, investment, insurance and payment services. Traditionally, financial services were primarily delivered through banks, insurance companies, stock exchanges and other regulated institutions operating through physical branches and established procedures. The development of internet banking, smartphones, digital payment platforms, artificial intelligence and cloud computing has changed this structure. Financial transactions that previously required physical documentation and personal visits can now be completed within minutes through digital platforms. Financial technology refers broadly to the use of technological innovation to develop, improve or deliver financial products and services. It includes mobile payment applications, digital lending platforms, online investment services, automated financial advice, electronic wallets, peer-to-peer lending and technology-supported insurance services. These innovations have contributed to financial inclusion by allowing individuals and small businesses to access services without depending entirely on conventional banking infrastructure.

In India, the growth of digital public infrastructure, electronic payment systems and mobile-based financial services has created opportunities for a wider section of the population to participate in the formal financial system. Digital transactions can reduce administrative costs, facilitate faster payments and support the development of small enterprises. Financial institutions can also use data analytics to assess creditworthiness, detect suspicious transactions and improve operational efficiency. However, the benefits of FinTech are accompanied by legal and economic risks. The rapid expansion of digital lending has raised concerns regarding excessive interest charges, misleading representations, unauthorised collection of personal information and coercive recovery practices. Cyberattacks, phishing, identity theft and payment fraud threaten the security of digital transactions. Automated decision-making may produce discriminatory outcomes, while excessive dependence on common cloud service providers can create operational vulnerabilities across several financial institutions simultaneously.

Another concern is the emergence of businesses that perform financial functions without being

directly regulated in the same manner as traditional financial institutions. A technology company may design a lending application, collect customer information, recommend financial products or facilitate transactions while a bank or non-banking financial company formally provides the underlying service. Such arrangements can make it difficult for consumers to identify the responsible entity and for regulators to determine the appropriate allocation of liability. Financial regulation is therefore necessary to establish minimum standards of conduct, define the responsibilities of market participants and provide effective remedies when financial services cause harm. Regulation also contributes to public confidence. Consumers are more likely to use digital financial products when they know that their money, personal information and legal rights receive adequate protection. Nevertheless, regulation must be designed carefully. Excessive compliance requirements may discourage smaller FinTech enterprises, increase operational costs and prevent useful innovations from reaching underserved communities. A regulatory framework that treats every technological business as if it were a bank may also impose inappropriate obligations. The central issue is therefore not whether FinTech should be regulated, but how financial regulation can respond effectively to changing business models without unnecessarily restricting innovation.

This article examines that issue through the Indian legal framework and relevant international regulatory principles. It contends that financial regulation in the FinTech era must combine consumer protection, technological resilience, institutional accountability and proportionate supervision.

IJLAR

Research Questions

The article addresses the following research questions:

1. Why is financial regulation necessary for the growth and responsible development of FinTech?
2. To what extent does the existing Indian legal and regulatory framework address the risks arising from technology-driven financial services?
3. What challenges arise in protecting consumers, maintaining cybersecurity and ensuring accountability in the FinTech ecosystem?
4. What legal and institutional reforms are required to balance financial innovation with consumer protection and financial stability?

Research Objectives

The principal objectives of the article are:

1. To examine the meaning, development and significance of FinTech in contemporary financial services.
2. To analyse the need for financial regulation in protecting consumers and maintaining confidence in digital financial transactions.
3. To evaluate the relevant Indian statutes, regulatory directions and institutional responsibilities governing FinTech activities.
4. To identify regulatory gaps concerning digital lending, data protection, cybersecurity, algorithmic decision-making and cross-border financial services.
5. To suggest legal and institutional measures that promote responsible innovation, regulatory coordination and effective accountability.

Research Methodology

The article adopts a doctrinal research methodology. It relies on primary sources, including Indian statutes, delegated legislation, regulatory directions and judicial decisions, together with secondary sources such as official reports, policy papers and academic publications. The analysis principally concerns the Indian jurisdiction, with comparative references to international regulatory developments where relevant. The research is analytical and evaluative rather than empirical. It examines whether the existing legal framework adequately addresses the risks associated with FinTech and identifies areas in which legislative or regulatory improvements may be necessary. The article does not claim to establish statistical relationships between FinTech adoption and financial misconduct; instead, it evaluates the legal principles and institutional arrangements relevant to responsible financial innovation.

1. FinTech and Its Development

1.1 Meaning and scope of FinTech

FinTech is not a single financial product or a separate category of institution. It is an umbrella term covering technologies used to provide, support or improve financial services. Its scope extends from simple electronic payment facilities to complex systems involving artificial intelligence, machine learning, distributed ledgers and automated financial decision-making. Digital payment applications enable the transfer of money between individuals and businesses. Digital lending platforms connect borrowers with lenders and may automate parts of the loan

application and assessment process. Robo-advisory services use algorithms to assist customers in making investment decisions. InsurTech enterprises use digital tools to distribute insurance, assess risks and process claims. RegTech and SupTech use technology to improve regulatory compliance and supervisory activities. These services do not necessarily fall under a single regulatory category. The applicable legal obligations depend on the financial activity, the nature of the entity, the product offered and the relevant statutory framework. A payment service, a securities investment platform and an insurance distribution service may involve different regulators and compliance requirements. This diversity makes a uniform, technology-only regulatory approach inadequate. A more effective framework must identify the underlying activity and the risks it creates before determining the appropriate regulatory obligations.

1.2 Benefits of FinTech

The principal benefit of FinTech is improved accessibility. Digital services can reduce geographical barriers and enable people in rural and semi-urban areas to access financial facilities. Small businesses may obtain payments and credit without depending exclusively on conventional banking channels. FinTech also improves speed and efficiency. Automated processes reduce paperwork, support faster settlement and allow institutions to monitor transactions in real time. Data-driven systems may improve fraud detection and help financial institutions evaluate applications more efficiently. Competition is another important benefit. New entrants can challenge established institutions by providing lower-cost services and more convenient customer experiences. Innovation may encourage traditional financial institutions to improve their services and develop more accessible products. Nevertheless, these benefits depend on appropriate governance. A digital platform that expands access to credit without assessing repayment capacity may contribute to excessive indebtedness. A payment service that prioritises speed without adequate security may expose customers to fraud. Innovation must therefore be accompanied by safeguards that preserve the integrity of the financial system.

1.3 FinTech and the changing nature of financial intermediation

Traditional financial regulation developed largely around identifiable institutions performing specific functions, such as accepting deposits, lending money, underwriting insurance and operating securities markets. FinTech introduces more complex arrangements in which several entities participate in a single transaction. For example, a customer seeking a digital loan may interact with an application developed by a technology company, provide information through

an intermediary and receive credit from a regulated lender. The lender may depend on external service providers for data processing, customer verification and loan servicing. This separation between the customer-facing platform and the entity providing the financial product can obscure responsibility. The customer may assume that the application itself is the lender, even though the legal relationship is with another entity. If a dispute arises, the customer may struggle to identify the appropriate authority or determine who is legally accountable. The Reserve Bank of India has recognised the importance of balancing financial innovation with customer protection, security, competition and risk management. Its regulatory approach increasingly addresses not only the regulated institution but also the outsourcing arrangements and technological infrastructure through which financial services are delivered.[1]

2. The Need for Financial Regulation in the FinTech Era

2.1 Protection of financial consumers

Consumer protection is one of the strongest justifications for financial regulation. Financial products can be complex, and customers may not possess the technical knowledge required to understand how digital platforms operate. Online interfaces can make transactions convenient, but they can also encourage customers to accept contractual terms without fully understanding the financial consequences. Digital lending illustrates this problem. Borrowers may be attracted by immediate loan approvals without adequately considering the annualised cost of borrowing, repayment obligations, late-payment consequences or data-sharing practices. Some unlawful or deceptive applications may falsely claim an association with regulated financial institutions. Regulation can address these risks through disclosure requirements, fair lending standards, restrictions on misleading representations and clear identification of the responsible lender. Customers should be informed of the total cost of credit, the identity of the lender, repayment schedules, applicable charges and available complaint mechanisms. The RBI's Digital Lending Directions, 2025, consolidate and develop the regulatory approach to digital lending, including concerns relating to third-party service providers, customer protection and the conduct of digital lending applications.[2] These directions demonstrate that technological delivery does not remove the legal responsibilities associated with lending. A central principle should be that the use of an intermediary must not weaken a consumer's legal protection. Where a regulated lender relies on an external platform to distribute or service a loan, regulatory accountability should

[1] Digitalisation and Financial Innovation, in Report on Currency and Finance (2023–24)
[2] Reserve Bank of India (Digital Lending) Directions, 2025.

remain clearly defined. Consumers should not be left without an effective remedy merely because a transaction involves several technological intermediaries.

2.2 Prevention of fraud and financial misconduct

Digital financial services expose customers to risks such as phishing, impersonation, fraudulent payment requests, account takeover and identity theft. Criminals may exploit the speed of electronic transactions and the difficulty of reversing payments after funds have been transferred. Traditional fraud prevention mechanisms are not always sufficient for these risks. Digital systems require continuous monitoring, authentication safeguards, secure communication and mechanisms to identify suspicious transaction patterns. Financial institutions must also ensure that customers receive timely warnings about emerging fraud techniques. Regulation can establish minimum security standards and require institutions to maintain internal controls, report relevant incidents and cooperate with competent authorities. It can also clarify responsibility where losses arise from failures in the design or operation of financial services. The RBI's regulatory framework for digital payment security controls and cyber resilience reflects the importance of technological safeguards in the payment ecosystem.[3] Such requirements are necessary because the failure of one service provider may affect a large number of transactions within a short period. However, regulation cannot eliminate every fraudulent transaction. Its purpose is to establish reasonable preventive standards, improve institutional preparedness and ensure that customers have accessible procedures for reporting and resolving disputes.

2.3 Maintenance of financial stability

Financial stability refers to the ability of the financial system to continue performing its essential functions despite economic shocks, operational disruptions or failures of individual institutions. FinTech can improve stability by strengthening risk assessment and operational efficiency, but it can also introduce new forms of interconnectedness. Several financial institutions may depend on the same cloud provider, payment processor, identity-verification service or software platform. A serious disruption affecting one common provider can therefore interrupt the services of numerous institutions simultaneously. This concentration risk may be overlooked if each institution is examined independently. Automated lending can also increase

[3] Reserve Bank of India, Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators (July 30, 2024).

correlated exposure. If multiple lenders use similar data sources and algorithms, they may respond to market changes in similar ways, potentially amplifying financial stress. Rapid digital transactions may accelerate withdrawals, transfers or changes in market positions during periods of uncertainty. The Financial Stability Board has examined the financial stability implications of FinTech and the importance of monitoring developments that may create vulnerabilities beyond individual firms.[4] The broader lesson is that financial regulation must assess not only the conduct of individual enterprises but also the systemic consequences of their interconnected activities. Regulators should therefore evaluate operational concentration, outsourcing dependencies, liquidity risks and the possible effects of technological failures on the wider financial system. Proportionate stress testing and business continuity planning can help reduce the likelihood that an isolated technological problem becomes a broader financial disruption.

2.4 Data privacy and responsible use of financial information

FinTech businesses often depend on extensive personal and financial data. Information concerning income, spending patterns, repayment history, location and digital behaviour may be used to assess creditworthiness, recommend products or detect fraud. Although data-driven systems can improve financial services, excessive or inappropriate collection may interfere with individual privacy. Customers may not understand how their information is obtained, combined, retained or shared with third parties. In some cases, access to a service may be made conditional on permissions that are broader than necessary for the transaction. The Digital Personal Data Protection Act, 2023, establishes an important statutory framework for the processing of digital personal data, subject to its provisions, applicable rules and commencement arrangements.[5] Its relevance to FinTech arises from the extensive processing of personal information by financial institutions and technology service providers. Financial regulation and data protection law serve related but distinct purposes. Financial regulation focuses on matters such as prudential soundness, market conduct and customer protection, whereas data protection law addresses the processing of personal data. Effective protection requires these frameworks to operate coherently. FinTech enterprises should collect information for specified purposes, adopt appropriate security measures, provide clear notices

[4] Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities' Attention (June 27, 2017).
[5] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

and respect applicable consent and other lawful processing requirements. Regulators should also consider whether the use of alternative data in lending creates risks of unfair exclusion or unjustified discrimination. Privacy protection should not be treated as an obstacle to innovation. Trustworthy data governance can improve customer confidence and reduce the legal and reputational costs of misuse.

2.5 Accountability in algorithmic decision-making

Artificial intelligence and machine learning are increasingly used in credit assessment, fraud detection, customer service and investment-related services. These systems can process large quantities of information and identify patterns that may be difficult to detect through manual analysis. However, algorithmic systems may produce inaccurate or discriminatory outcomes. A credit model trained on historical data may reproduce existing social or economic inequalities. An automated system may reject a loan application without providing the customer with a meaningful explanation. Errors in the underlying data may also affect decisions concerning credit limits, interest rates or fraud alerts. The legal challenge is to identify responsibility when a decision is generated through a complex technological process. A financial institution cannot adequately protect itself or its customers merely by asserting that a decision was made by an algorithm or an external vendor. Institutions should maintain appropriate documentation, test systems for reliability and bias, establish human review procedures for significant adverse decisions and provide channels for customers to challenge errors. The degree of explanation and human oversight should reflect the significance of the decision and the risks involved. International policy analysis also highlights the need to supervise artificial intelligence in finance while preserving innovation and protecting consumers.[6] In the Indian context, regulators should develop risk-based expectations for algorithmic governance, particularly where automated systems materially affect access to credit, investment services or other essential financial products.

2.6 Prevention of regulatory arbitrage

Regulatory arbitrage occurs when businesses structure their activities to obtain a commercial advantage by avoiding or minimising applicable regulatory obligations. FinTech can increase this risk because technological enterprises may perform functions traditionally associated with regulated institutions without adopting the same legal form. For instance, a business may

[6] Regulatory Approaches to Artificial Intelligence in Finance, OECD Artificial Intelligence Papers No. 24 (2024)

facilitate lending through a digital platform while presenting itself primarily as a technology intermediary. The regulatory position depends on the actual activity, applicable law and contractual arrangements, not merely on the description used by the business. If similar financial activities are subject to substantially different standards solely because one provider uses a digital platform, competition may become distorted. Customers may also face weaker protection when services are provided outside a clearly defined regulatory perimeter. Regulation should therefore be based substantially on the nature, scale and risk of the activity. Businesses performing equivalent financial functions should be subject to appropriately comparable safeguards, while obligations should remain proportionate to their actual responsibilities. This approach does not mean that every technology provider should be licensed as a bank. Instead, it requires a clear distinction between purely technical services and activities involving the provision, arrangement, control or distribution of regulated financial products.

2.7 Financial inclusion and responsible innovation

Financial regulation is sometimes criticised for increasing compliance costs and slowing innovation. This concern is particularly relevant to smaller enterprises that lack the resources of established financial institutions. Poorly designed regulation may reduce competition and limit access to services for underserved groups. Nevertheless, the absence of regulation can also undermine inclusion. Fraud, unfair lending and misuse of customer information disproportionately affect individuals who have limited financial knowledge or few alternative service providers. A loss of trust may discourage people from using formal digital financial services. The appropriate objective is therefore responsible financial inclusion. Regulation should distinguish between risks that require strict controls and activities that can operate under simplified requirements. Small-scale innovation may be supported through regulatory sandboxes, controlled pilots and proportionate reporting obligations. The RBI's regulatory sandbox framework provides a mechanism through which eligible financial innovations can be tested under specified conditions.[7] Such mechanisms allow regulators to understand emerging technologies before deciding whether existing rules require clarification or amendment. Innovation should be encouraged where it improves access, affordability and service quality. However, commercial experimentation should not remove essential protections concerning customer consent, security, truthful disclosures and the handling of complaints.

[7] Reserve Bank of India, Enabling Framework for Regulatory Sandbox (Feb. 2024).

3. The Indian Legal and Regulatory Framework Governing FinTech

3.1 The Reserve Bank of India and banking regulation

The RBI is the principal regulatory authority for banking and several categories of payment and credit-related activities in India. Its statutory powers derive from legislation including the Reserve Bank of India Act, 1934, and the Banking Regulation Act, 1949.[8] These statutes provide the legal foundation for monetary and banking functions, regulatory directions and supervision within their respective scopes. The RBI's role has expanded in practical importance as financial institutions increasingly rely on digital channels and external technology providers. Its regulatory responsibilities include addressing risks associated with payment systems, digital lending, outsourcing, information technology and customer service. The Payment and Settlement Systems Act, 2007, provides the statutory framework for the regulation and supervision of payment systems. [9]This is particularly significant because electronic payments depend on reliable infrastructure, secure processing and effective arrangements among participating entities. Regulatory directions issued under the applicable statutes can establish operational requirements that respond more quickly to technological developments than primary legislation alone. However, delegated regulation must remain within statutory authority and be applied consistently with principles of legality and procedural fairness.

3.2 Regulation of digital lending

Digital lending presents a useful example of how financial regulation must adapt to new business models. The rapid processing of loan applications can improve access to credit, but customers may be exposed to misleading representations, unclear charges, inappropriate data collection and aggressive recovery practices. The RBI's Digital Lending Directions, 2025, provide a consolidated framework governing relevant digital lending activities of regulated entities. They address issues associated with lending service providers, digital lending applications and the responsibilities of regulated lenders.[10] The framework is significant because outsourcing does not, by itself, eliminate the lender's regulatory obligations. A sound regulatory approach requires borrowers to receive clear information about the identity of the lender, the financial terms of the loan and the mechanisms available for complaints. It should also ensure that the handling of personal data and the conduct of recovery activities remain

[8] Reserve Bank of India Act, No. 2 of 1934, India Code; Banking Regulation Act, No. 10 of 1949, India Code.
[9] Payment and Settlement Systems Act, No. 51 of 2007, India Code.
[10] Reserve Bank of India, Reserve Bank of India (Digital Lending) Directions, 2025.

consistent with applicable legal requirements. The effectiveness of these directions depends on implementation, supervision and enforcement. Authorities must be capable of identifying unlawful applications, examining arrangements between lenders and intermediaries and responding promptly to complaints involving serious misconduct.

3.3 Securities regulation and digital investment services

FinTech has also transformed investment services through online trading platforms, digital investment interfaces, algorithmic tools and automated portfolio services. These developments may widen market participation, but they also create risks involving misleading investment claims, unsuitable products, market manipulation and the misuse of customer information. The Securities and Exchange Board of India Act, 1992, establishes SEBI and provides its statutory foundation.[11] The Securities Contracts (Regulation) Act, 1956, and the Depositories Act, 1996, form additional parts of the legal framework governing securities markets and associated infrastructure.[12] SEBI's regulatory responsibilities are relevant where technology-enabled services involve securities markets, intermediaries, investor-facing recommendations or other activities within its jurisdiction. Digital delivery does not exempt a market participant from applicable securities laws. Investors should receive adequate disclosures concerning financial products, charges and material risks. Platforms should not make misleading claims about guaranteed returns or conceal conflicts of interest. Automated investment services should also be subject to appropriate standards concerning suitability, transparency and accountability, depending on their regulatory classification. The regulatory objective should be to preserve the accessibility of digital investment services while ensuring that technological convenience does not weaken investor protection or market integrity.

3.4 Insurance technology and regulatory supervision

Technology has influenced insurance distribution, underwriting, claims management and customer service. Digital insurance platforms can reduce transaction costs and improve access to products. Data analytics may also help insurers assess risk and identify fraudulent claims. At the same time, technology-driven insurance services raise questions concerning disclosure, fairness in risk assessment, data security and the handling of rejected claims. Customers may find it difficult to understand how automated decisions influence premiums or eligibility. The

[11] Securities and Exchange Board of India Act, No. 15 of 1992, India Code.
[12] Securities Contracts (Regulation) Act, No. 42 of 1956, India Code; Depositories Act, No. 22 of 1996, India Code.

Insurance Regulatory and Development Authority of India Act, 1999, provides the statutory foundation for insurance regulation in India.[13] The IRDAI supervises insurance-sector activities within its statutory mandate, including relevant aspects of insurer conduct and policyholder protection. Where insurance is distributed through digital intermediaries, responsibilities should be clearly allocated among insurers, distributors and technology service providers. Customers must be able to identify the insurer, understand policy exclusions and access complaint mechanisms. Insurance regulation should also examine whether data-driven pricing and automated underwriting produce outcomes inconsistent with applicable law or established standards of fair treatment.

3.5 Data protection and information technology law

The legal framework for FinTech must address both the financial transaction and the technological systems supporting it. The Information Technology Act, 2000, provides a statutory framework for electronic records, electronic transactions and specified cyber-related offences and liabilities.[14] Its provisions may be relevant where digital financial activities involve unauthorised access, interference with computer resources or other conduct covered by the Act. The Digital Personal Data Protection Act, 2023, addresses the processing of digital personal data within its scope.[15] Together with applicable rules and other relevant laws, it forms part of the legal environment in which financial institutions and technology providers must operate. However, legal compliance cannot be achieved merely by publishing a privacy policy or obtaining a general customer acceptance. Organisations must implement appropriate governance arrangements, control access to sensitive information and ensure that data-processing practices comply with the applicable statutory requirements. Financial regulators and data protection authorities should coordinate where an incident simultaneously involves a financial service failure, unauthorised access to personal data and consumer harm. Clear institutional procedures can reduce duplication and prevent disputes over regulatory responsibility.

3.6 Consumer protection and grievance redressal

Digital financial services are also subject to applicable consumer protection principles. The Consumer Protection Act, 2019, provides a framework addressing consumer rights and

[13] Insurance Regulatory and Development Authority of India Act, No. 41 of 1999, India Code.
[14] Information Technology Act, No. 21 of 2000, India Code.
[15] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

specified forms of unfair trade practices and deficiency in services.[16] Its application depends on the nature of the transaction, the parties involved and the statutory requirements. A customer who experiences a disputed transaction, misleading representation or deficient financial service should be able to identify the appropriate complaint channel. Fragmented procedures can create confusion, especially where the service provider, payment intermediary and financial institution are different entities. Sector-specific grievance mechanisms are important, but they must be understandable and accessible. Customers should receive acknowledgement of complaints, information about expected timelines and reasons for the decisions reached. Where a matter falls within the applicable framework of the RBI's Integrated Ombudsman Scheme, eligible customers may use that mechanism after satisfying the relevant conditions.[17] Other disputes may require recourse to the appropriate regulator, consumer commission, law enforcement authority or court. Effective grievance redressal is essential because the practical value of consumer rights depends on whether customers can enforce them without unreasonable cost or delay.

3.7 Self-regulation and industry standards

Government regulation alone may not always respond quickly enough to the changing technological landscape. Industry bodies can contribute by developing technical standards, ethical guidelines, training requirements and mechanisms for resolving certain industry-level concerns. In May 2024, the RBI issued a framework for recognising self-regulatory organisations in the FinTech sector.[18] The framework reflects the potential role of industry-level institutions in promoting responsible conduct and improving communication between market participants and regulators. Self-regulation, however, must supplement rather than replace statutory supervision. Industry members may have commercial interests that conflict with consumer protection, and voluntary standards may not provide adequate remedies for serious misconduct. An effective arrangement should combine regulatory oversight with transparent governance, independent complaint handling and clear consequences for non-compliance. Recognised self-regulatory organisations should also operate within defined limits and remain accountable to the relevant regulator. The aim is to use industry expertise to improve regulatory effectiveness without allowing private bodies to determine the scope of public legal obligations.

[16] Consumer Protection Act, No. 35 of 2019, India Code.
[17] Reserve Bank of India, Reserve Bank—Integrated Ombudsman Scheme, 2021
[18] Reserve Bank of India, Framework for Self-Regulatory Organisation(s) in the FinTech Sector (May 30, 2024).

4.Major Regulatory Challenges in the FinTech Ecosystem

4.1 Fragmented regulatory supervision

FinTech activities may fall within the jurisdiction of different authorities depending on whether they involve banking, payment systems, securities, insurance or data processing. This sector-specific arrangement reflects the different risks associated with financial products. However, a single digital service may combine several regulated activities. A platform may facilitate payments, offer access to credit and distribute investment products through the same interface. If the relevant authorities apply inconsistent standards or fail to share information, gaps in supervision may arise. The solution is not necessarily to establish one regulator for every FinTech activity. Such a move could disrupt existing institutional expertise. Instead, clear coordination procedures, information-sharing arrangements and joint responses to cross-sector risks are required. Regulatory coordination should also identify which authority has primary responsibility for particular complaints and incidents. A consumer should not be required to understand the entire regulatory structure before reporting a financial loss.

4.2 Cybersecurity and third-party dependence

Digital financial services depend on software systems, data centres, communication networks and external service providers. A security failure in any part of this infrastructure may affect the confidentiality, availability or integrity of financial information. Third-party dependence creates a special challenge because regulated institutions may not directly control every technological component of their operations. Contracts can allocate responsibilities between businesses, but they cannot alone ensure effective supervision or protect customers against every operational failure. Institutions should conduct risk assessments before engaging technology providers, monitor critical service arrangements and maintain practical contingency plans. Outsourcing contracts should establish security requirements, incident reporting procedures, access to relevant records and cooperation with regulatory investigations. Supervisory authorities should also evaluate concentration risks where several institutions depend on the same provider. Operational resilience must be considered a core element of financial regulation rather than merely an internal information technology concern.

4.3 Cross-border transactions and jurisdiction

Digital financial services can operate across national borders without requiring a physical presence in every jurisdiction in which customers are located. This creates questions

concerning licensing, consumer remedies, data transfers, evidence collection and enforcement. A fraudulent platform may target customers in one country while operating through servers, intermediaries and corporate entities in several others. Determining the responsible entity and securing relevant records may require cooperation between different authorities. Cross-border regulatory cooperation is therefore essential. Regulators should develop procedures for sharing information, investigating misconduct and responding to significant cybersecurity incidents, subject to applicable law and safeguards for confidential information. International standards can support greater consistency, but they cannot replace domestic legal authority. Indian regulators must ensure that cross-border arrangements remain compatible with Indian statutes and the legitimate interests of domestic consumers.

4.4 Regulatory uncertainty and compliance costs

Uncertainty about the legal classification of a new service can discourage investment and make compliance difficult. A FinTech enterprise may be unsure whether its activities amount to the provision of a regulated financial service, an outsourced function or a purely technical service. Unclear requirements may also produce inconsistent treatment of similar business models. Large institutions may be able to absorb the cost of obtaining legal advice and maintaining complex compliance systems, while smaller firms may struggle to meet the same administrative burden. Regulators should provide accessible guidance, clarify the scope of applicable requirements and consult relevant stakeholders when developing new standards. Proportionate obligations can distinguish between enterprises according to the nature of their activities, their exposure to customer funds and the risks they create. Regulatory flexibility should not mean that businesses can avoid essential protections. Rather, it should ensure that compliance requirements are directed towards identifiable risks and remain proportionate to the activities being regulated.

4.5 Artificial intelligence, discrimination and explainability

Algorithmic decision-making presents difficult questions of accountability because the reasons behind a decision may not be easily understood by a customer or even by the institution using the system. A model may rely on inaccurate data, reproduce historical inequalities or generate results that vary significantly across customer groups. If the system is used to assess creditworthiness, errors may restrict access to financial services or impose unfair costs. Financial institutions should retain responsibility for decisions made through systems deployed

in their operations. This requires suitable validation, monitoring, documentation and human oversight. Customers should have meaningful avenues to correct inaccurate information and challenge material errors. Regulators must also recognise that complete technical disclosure is not always necessary or appropriate. The objective should be meaningful accountability: sufficient information for supervisors to assess compliance and for affected customers to understand and challenge consequential decisions.

4.6 Unequal access and digital literacy

The growth of digital finance does not automatically guarantee financial inclusion. Individuals may lack reliable internet access, suitable devices or the knowledge required to recognise fraudulent communications. Persons with disabilities and customers who are unfamiliar with digital interfaces may face additional barriers. An exclusively digital system may also disadvantage customers who require assistance or cannot complete electronic verification procedures. Financial regulation should therefore consider accessibility, alternative service channels and clear communication. Financial literacy initiatives should explain the risks associated with sharing authentication credentials, accepting loan offers and responding to suspicious payment requests. Consumer education should complement, rather than replace, the legal obligations of financial service providers. Responsible regulation should ensure that technological progress expands access to financial services without making meaningful participation dependent on advanced digital skills.

5. Comparative and International Perspectives

5.1 International principles for FinTech regulation

FinTech operates in a global environment, and many of its risks are not confined to one jurisdiction. Cybersecurity incidents, technology dependencies, cross-border payments and digital investment services may involve multiple countries. International regulatory principles can therefore help national authorities develop compatible approaches. The Financial Stability Board has examined the implications of FinTech for financial stability, including developments that may affect established regulatory frameworks.[19] The Basel Committee on Banking Supervision has also considered how technological innovation changes banking business

[19] Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities' Attention (June 27, 2017).

models and the associated risks.[20] These institutional assessments support a risk-based approach that focuses on the financial activity and its consequences rather than on technology alone. International cooperation is particularly relevant when a technology provider operates across several jurisdictions. Common principles concerning operational resilience, governance and disclosure can reduce inconsistent expectations and support effective supervision. However, international guidance must be adapted to domestic circumstances. India's financial system includes a large population of small customers and enterprises, varied levels of digital literacy and a regulatory structure shaped by domestic statutes. Imported models should therefore be assessed against local legal requirements and practical needs.

5.2 Regulatory sandboxes and innovation

Regulatory sandboxes allow eligible firms to test innovative products or services within a controlled environment and subject to specified conditions. They can help regulators understand the practical operation of new technologies and identify risks before wider deployment. The United Kingdom's Financial Conduct Authority has developed a regulatory sandbox approach intended to facilitate controlled testing of financial innovations. [21] Such approaches demonstrate how regulatory supervision can support experimentation without abandoning safeguards. India can benefit from similar mechanisms where they are carefully designed and transparently administered. Eligibility criteria, testing conditions, customer safeguards and reporting obligations should be clear. Participation should not be understood as a general exemption from applicable law, nor should it imply that the regulator guarantees the commercial success or safety of a product. Sandboxes are most useful when their findings inform future regulatory decisions. Lessons concerning consumer behaviour, security weaknesses and compliance difficulties should be evaluated to determine whether broader guidance or regulatory changes are warranted.

5.3 Regulatory technology and supervisory technology

Regulatory technology, commonly known as RegTech, uses digital tools to assist financial institutions in meeting compliance obligations. Supervisory technology, or SupTech, uses technological systems to support the work of regulators. RegTech applications may automate reporting, monitor transactions and identify compliance anomalies. SupTech systems may help

[20] Basel Comm. On Banking Supervision, Sound Practices: Implications of FinTech Developments for Banks and Bank Supervisors (Feb. 2018).

regulators analyse large volumes of information, identify patterns across institutions and prioritise supervisory investigations. These tools can improve efficiency, but they introduce their own risks. Automated monitoring may produce false positives, and poorly designed systems may overlook unusual misconduct. Excessive dependence on automated supervision may also obscure the reasons for a regulatory decision. Regulators should therefore combine technological tools with expert review, appropriate validation and clear accountability. The purpose of RegTech and SupTech should be to strengthen human and institutional judgment, not to replace it entirely.

6. Suggestions and Recommendation

The Indian financial regulatory framework should be strengthened to address the emerging challenges associated with FinTech while encouraging responsible technological innovation. First, there is a need for better coordination among the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority of India (IRDAI), and other relevant authorities. A coordinated regulatory mechanism would help reduce overlapping jurisdiction, prevent regulatory gaps and ensure consistent supervision of financial services offered through digital platforms. Regulatory obligations should be based on the nature of the financial activity and the risks involved rather than merely on the technological model adopted by the service provider. Secondly, consumer protection must be given greater importance in digital financial transactions. FinTech companies and regulated financial institutions should provide clear information regarding interest rates, processing charges, repayment conditions, investment risks and the identity of the entity responsible for providing the service. In digital lending, borrowers should be protected against misleading advertisements, hidden charges, unlawful recovery practices and unauthorised collection of personal information. Effective grievance redressal mechanisms should be established to enable customers to report fraudulent transactions, obtain timely responses and seek appropriate remedies without unnecessary procedural difficulties. Thirdly, stronger cybersecurity and data protection measures should be implemented to protect financial information and prevent digital fraud. Financial institutions should conduct regular security assessments, adopt appropriate authentication mechanisms, monitor suspicious transactions and maintain effective incident-response procedures. They should also ensure that third-party technology providers comply with applicable security requirements. Personal and financial information should be collected and processed only in accordance with applicable law, with

appropriate safeguards against unauthorised access, disclosure and misuse. Cooperation between financial regulators and data protection authorities should be strengthened to address incidents involving both financial loss and violations of privacy. Fourthly, appropriate regulatory standards should be developed for the use of artificial intelligence and automated decision-making in financial services. Institutions using algorithmic systems for credit assessment, fraud detection or investment-related decisions should ensure that such systems are reliable, adequately tested and regularly monitored. Where automated decisions materially affect customers, suitable mechanisms should be available for human review, correction of inaccurate information and challenge of unfair outcomes. Financial institutions should remain accountable for decisions made through technologies used in their operations and should not avoid responsibility by attributing errors entirely to automated systems or external service providers. Fifthly, the regulatory framework should promote innovation through regulatory sandboxes and proportionate compliance requirements. Start-ups and smaller FinTech enterprises should receive clear regulatory guidance and opportunities to test innovative products under controlled conditions. However, such flexibility should not compromise essential standards of consumer protection, cybersecurity, transparency or financial stability. Periodic review of regulatory directions would help authorities respond to technological developments and remove unnecessary compliance burdens while maintaining effective safeguards. Finally, financial literacy, international cooperation and effective enforcement should be strengthened. Government authorities, educational institutions and financial service providers should educate the public about digital payment safety, online lending risks, investment fraud and the protection of authentication credentials. Regulatory authorities should also improve cooperation with foreign counterparts to address cross-border fraud, cybercrime and disputes involving international technology providers. At the same time, violations of financial regulations should attract proportionate and effective enforcement action. A balanced, transparent and adaptable regulatory framework is essential to ensure that FinTech promotes financial inclusion and economic development without weakening consumer rights, data privacy or the stability of the financial system.

7. Conclusion

The rapid development of financial technology has brought significant changes to the financial sector by improving the accessibility, efficiency, speed and affordability of financial services. Digital payments, online lending, mobile banking, automated investment services and artificial

intelligence have created new opportunities for financial inclusion and economic growth. However, these advancements have also introduced serious challenges relating to consumer protection, cybersecurity, data privacy, financial fraud, algorithmic discrimination and financial stability. The present study demonstrates that financial regulation is essential to ensure that technological innovation operates within a clear and accountable legal framework. In India, institutions such as the Reserve Bank of India, the Securities and Exchange Board of India and the Insurance Regulatory and Development Authority of India play important roles in supervising financial activities within their respective jurisdictions. Although existing legislation and regulatory directions provide a foundation for addressing FinTech-related risks, continuous improvements are necessary to respond to emerging technologies, complex business models and cross-border transactions. Greater coordination among regulatory authorities, stronger cybersecurity standards, transparent digital lending practices, responsible use of personal data, effective grievance redressal mechanisms and appropriate oversight of artificial intelligence are essential to strengthen public confidence in digital financial services. Furthermore, regulatory sandboxes, proportionate compliance requirements and financial literacy programmes can encourage innovation while ensuring adequate protection for consumers and investors. Financial regulation should not be viewed as an obstacle to technological advancement; rather, it should serve as a mechanism for ensuring that innovation develops responsibly and sustainably. Therefore, the need for financial regulation in the era of FinTech lies in achieving a proper balance between innovation, consumer protection, market integrity and financial stability. A transparent, flexible and risk-based regulatory framework will enable India to realise the benefits of financial technology while minimising its associated risks and promoting an inclusive, secure and trustworthy financial ecosystem.

REFERENCES

A. *Books:*

1. Douglas W. Arner, Janos Barberis & Ross P. Buckley, The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries (Wiley 2019).
2. Chris Skinner, Digital Bank: Strategies to Launch or Become a Digital Bank (Marshall Cavendish Business 2014).
3. Susanne Chishti & Janos Barberis eds., The FINTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries (Wiley 2016).

4. David Lee Kuo Chuen & Robert H. Deng eds., Handbook of Blockchain, Digital Finance, and Inclusion (Academic Press 2018).

B. *Reports and Research Publications:*

1. Basel Comm. On Banking Supervision, Sound Practices: Implications of FinTech Developments for Banks and Bank Supervisors (Bank for Int'l Settlements 2018).
2. Fin. Stability Bd., Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities' Attention (2017).
3. Int'l Org. Of Sec. Comm'n, Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges (2025).
4. Org. For Econ. Co-operation & Dev., Regulatory Approaches to Artificial Intelligence in Finance (OECD Artificial Intelligence Papers No. 24, 2024).
5. Org. For Econ. Co-operation & Dev., Supervision of Artificial Intelligence in Finance: Challenges, Policies and Practices (OECD Artificial Intelligence Papers No. 54, 2026).
6. Reserve Bank of India, Report of the Working Group on Digital Lending Including Lending Through Online Platforms and Mobile Apps (2021).
7. Reserve Bank of India, Report on Currency and Finance 2023–24 (2024).
8. World Bank, The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19 (2022).
9. World Bank, Fintech and the Future of Finance: Market and Policy Implications (2022).

C. *Statutes and Legislations :*

Reserve Bank of India Act, No. 2 of 1934, India Code. Banking Regulation Act, No. 10 of 1949, India Code.

Securities Contracts (Regulation) Act, No. 42 of 1956, India Code. Securities and Exchange Board of India Act, No. 15 of 1992, India Code.

Insurance Regulatory and Development Authority of India Act, No. 41 of 1999, India Code. Information Technology Act, No. 21 of 2000, India Code.

Payment and Settlement Systems Act, No. 51 of 2007, India Code. Consumer Protection Act, No. 35 of 2019, India Code.

Digital Personal Data Protection Act, No. 22 of 2023, India Code. Depositories Act, No. 22 of 1996, India Code.

D. *Webliography:*

https://m.rbi.org.in

https://littdb.sfo2.cdn.digitaloceanspaces.com/litt/IN/RBI/notifications/

https://financialservices.gov.in/

https://www.worldbank.org/en/publication/globalfindex.

https://www.iosco.org/

https://www.oecd.org/en https://www.bis.org/

IJLAR