Anusandhanvallari
Vol 2024, No.1
November 2024
ISSN 2229-3388

Fintech Revolution and the Future of E-Banking Laws in India

Mr. Subham Chatterjee[1], Mr. Amrita Dasgupta[1], Mr. Kaji Mainuddin[2]

[1] Assistant Professor, School of Law, Brainware University, Kolkata

[2]Research Scholar, Department of Law, University of Calcutta

Abstract

The rapid expansion of Financial Technology (FinTech) has fundamentally transformed the structure and delivery of banking services in India. Digital payment systems, mobile banking platforms, algorithm-driven lending, and data-centric financial services have enhanced financial inclusion and efficiency at an unprecedented scale. However, this transformation has simultaneously exposed structural inadequacies in the legal framework governing e-banking. This paper critically examines the evolution of e-banking laws in India, evaluates the regulatory role of the Reserve Bank of India (RBI), and identifies key legal challenges relating to data protection, cybersecurity, liability, and regulatory fragmentation. By integrating judicial precedents such as *Justice K.S. Puttaswamy v. Union of India*, *Internet and Mobile Association of India v. RBI*, and *Anvar P.V. v. P.K. Basheer*, the study situates FinTech regulation within a broader constitutional and evidentiary framework. Further, by incorporating empirical fraud statistics and real-world Indian case studies, the paper demonstrates that digital financial fraud is not incidental but systemic. A comparative analysis with global frameworks highlights India's strengths in adoption alongside its regulatory limitations. The paper argues for a transition toward anticipatory, ecosystem-based regulation to ensure the sustainable and secure growth of digital banking in India.

Keywords: FinTech, e-banking, RBI, digital payments, cybersecurity, privacy, regulation

1. Introduction

The integration of digital technologies into financial services has brought about a profound structural transformation in the Indian banking ecosystem. What was once a predominantly branch-based, paper-dependent, and time-bound system has increasingly evolved into a platform-driven, data-intensive, and real-time financial network. The rise of Financial Technology (FinTech) has played a central role in this transition, fundamentally altering how financial services are produced, delivered, and consumed (Arner et al., 2016). Innovations such as the Unified Payments Interface (UPI), mobile wallets, internet banking applications, and artificial intelligence-based financial tools have redefined how individuals' access, manage, and transfer money. Banking is no longer confined to physical branches or limited by operational hours; rather, it is embedded within digital platforms that enable users to perform financial transactions instantaneously. India today stands as one of the largest digital payment markets globally, processing billions of transactions every month through interoperable systems governed by the Reserve Bank of India (RBI, 2007).

This transformation has yielded substantial benefits, particularly in advancing financial inclusion and operational efficiency. Digital financial systems have extended banking access to previously underserved populations, especially in semi-urban and rural areas, thereby integrating a larger segment of society into the formal financial system. Moreover, FinTech innovations have significantly reduced transaction costs, improved speed, and enhanced transparency in financial dealings (Gomber et al., 2017). Real-time settlement systems such as UPI have enabled seamless interactions between banks, payment service providers, merchants, and

consumers, contributing to a more dynamic and accessible financial ecosystem. In this sense, FinTech has not merely modernized banking practices but has reshaped the underlying architecture of financial governance in India.

However, the rapid pace of technological advancement has also exposed critical deficiencies in the legal and regulatory framework governing e-banking. Much of India's financial legislation, including the Information Technology Act, 2000 and the Payment and Settlement Systems Act, 2007, was enacted in a pre-FinTech era and does not adequately address the complexities of contemporary digital finance (Government of India, 2000; RBI, 2007). Modern financial systems involve multi-party transaction chains, algorithm-driven decision-making, and real-time financial operations that challenge traditional legal concepts of liability, consent, and accountability. The increasing reliance on data-centric financial services has further intensified concerns regarding privacy and data protection, particularly in light of the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017).

This paper proceeds from the argument that the FinTech revolution has created a structural mismatch between technological capability and legal regulation in India. The issue is not merely one of regulatory delay but of conceptual inadequacy, where existing legal frameworks are ill-suited to govern digitally mediated financial systems. Through doctrinal analysis, judicial interpretation, and empirical examination of fraud trends and regulatory responses, this study seeks to identify the nature and extent of this mismatch. It ultimately proposes a forward-looking, adaptive, and technology-sensitive regulatory framework capable of balancing innovation with consumer protection, institutional accountability, and systemic stability in the evolving landscape of Indian e-banking.

2. Evolution of E-Banking Laws in India

The legal framework governing e-banking in India has developed in a largely incremental and reactive manner, rather than through a cohesive and forward-looking legislative strategy. One of the earliest and most significant statutory interventions in this domain was the enactment of the Information Technology Act, 2000, which granted legal recognition to electronic records and digital signatures, thereby facilitating the growth of e-commerce and online banking (Government of India, 2000). This legislation marked a foundational shift by enabling electronic transactions to carry the same legal validity as paper-based documentation. However, despite its pioneering role, the Act remains limited in its scope, as it was designed in a pre-FinTech era and does not adequately address contemporary challenges such as algorithmic decision-making, artificial intelligence in financial services, or the governance of platform-based financial ecosystems (Arner et al., 2016).

Parallel to this, the traditional banking sector in India continues to be governed by legacy statutes such as the Banking Regulation Act, 1949 and the Reserve Bank of India Act, 1934, which primarily focus on the regulation, supervision, and licensing of banking institutions. These statutes were formulated in an era when banking activities were institution-centric and conducted through physical infrastructure. As a result, they do not sufficiently account for the role of FinTech entities, which now function as critical intermediaries in financial transactions without necessarily being classified as banks. This creates a regulatory gap, as many FinTech firms operate in a hybrid space between technology and finance, often falling outside the direct purview of traditional banking laws (Gomber et al., 2017).

A more contemporary legislative effort is reflected in the Payment and Settlement Systems Act, 2007, which empowers the Reserve Bank of India (RBI) to regulate and supervise payment systems in the country (Reserve Bank of India, 2007). This Act has played a crucial role in enabling the development of digital payment infrastructures such as NEFT, RTGS, and, more recently, UPI, which forms the backbone of India's digital

payment ecosystem. While the Act provides a regulatory foundation for payment systems, it does not fully capture the complexities introduced by private FinTech platforms, including issues related to interoperability, data sharing, cross-platform transactions, and third-party service providers.

In the absence of a comprehensive legislative framework, the RBI has increasingly relied on regulatory guidelines and circulars to address emerging challenges in e-banking. Notable among these are the 2017 circular on limiting customer liability in unauthorized electronic transactions and the 2022 guidelines on digital lending, which aim to enhance consumer protection and regulate FinTech-driven credit systems (Reserve Bank of India, 2017; Reserve Bank of India, 2022). While these measures represent important steps toward addressing specific risks, they remain largely reactive and fragmented in nature. They are often introduced in response to emerging issues rather than as part of a unified regulatory vision.

This fragmented and piecemeal approach underscores the absence of a comprehensive FinTech regulatory framework in India. As digital financial systems continue to evolve in complexity and scale, there is an increasing need for a cohesive legal architecture that integrates statutory law, regulatory oversight, and technological realities. Without such integration, the existing framework risks becoming inadequate for governing the rapidly transforming landscape of e-banking in India.

3. Rise of FinTech in India

The growth of Financial Technology (FinTech) in India has been driven by a convergence of technological innovation, proactive policy support, and widespread digital penetration. Government initiatives such as Digital India, coupled with the rapid expansion of smartphone usage and affordable internet access, have created a fertile environment for digital financial services. Among these developments, digital payment systems—particularly the Unified Payments Interface (UPI)—have played a transformative role by enabling real-time, low-cost, and interoperable transactions across banks and platforms (Reserve Bank of India [RBI], 2007). UPI has not only enhanced transactional efficiency but has also significantly contributed to financial inclusion by allowing individuals without traditional banking access to participate in the digital economy.

Beyond payments, the FinTech ecosystem in India encompasses a wide range of services, including digital lending platforms, neo-banks, robo-advisory systems, and artificial intelligence (AI)-driven financial tools. These innovations have blurred the traditional boundaries between regulated banking institutions and technology firms, resulting in hybrid financial ecosystems where services are often delivered through partnerships between banks and FinTech companies (Arner et al., 2016). While this integration has expanded access to credit and financial services, it has also raised critical concerns regarding transparency, accountability, and consumer protection. The absence of clear regulatory categorization for such hybrid entities complicates oversight and creates potential risks for users (Gomber et al., 2017).

Artificial intelligence has further enhanced the efficiency of financial services by enabling automated credit scoring, fraud detection, and personalized financial recommendations. However, the reliance on algorithmic decision-making introduces concerns about bias, opacity, and lack of explainability in financial outcomes. Decisions regarding loan approvals or risk assessments may be influenced by opaque models, making it difficult for consumers to understand or challenge adverse outcomes. Similarly, the rapid expansion of digital lending platforms has improved access to credit, particularly for underserved populations, but has also been associated with predatory practices, excessive interest rates, and misuse of personal data. These issues highlight the dual nature of FinTech innovation: while it democratizes access to financial services, it simultaneously introduces new forms of systemic risk that require careful regulatory intervention.

4. Key Legal Challenges

India's FinTech and e-banking landscape is shaped by rapid innovation, but the legal structure governing it remains uneven and fragmented. A major reason is that regulation is distributed across multiple institutions rather than consolidated within a single, unified framework. Bodies such as the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Ministry of Electronics and Information Technology (MeitY), the National Payments Corporation of India (NPCI), and, in some contexts, the Competition Commission of India (CCI) and the Ministry of Finance each supervise different parts of the digital financial ecosystem. RBI oversees banks, payment systems, and certain banking-linked digital lending activities; SEBI regulates market-linked financial products; MeitY handles digital governance and cybersecurity issues; and NPCI manages payment rails such as UPI. While this structure reflects the multi-dimensional nature of FinTech, it also produces overlap, uncertainty, and regulatory gaps. A single service may simultaneously fall under banking regulation, technology regulation, and quasi-regulatory oversight, making compliance burdensome and enforcement inconsistent.

Data protection and privacy form another critical concern. FinTech platforms rely heavily on personal and financial data, including transaction histories, identity credentials, location data, behavioral patterns, and credit profiles. The Supreme Court's ruling in *Justice K.S. Puttaswamy v. Union of India* (2017) gave constitutional recognition to privacy as a fundamental right, thereby strengthening the legal basis for protecting consumer financial data. Yet constitutional recognition has not translated into sufficiently robust sector-specific safeguards in digital finance. Important questions remain unresolved regarding data minimization, purpose limitation, profiling, informed consent, and liability for misuse of information by intermediaries or third-party service providers. Weak privacy governance can expose consumers to surveillance, manipulation, and exploitative profiling, making privacy not only a rights-based issue but also a question of institutional trust.

Cybersecurity risks have expanded alongside the growth of digital banking. The increased use of app-based transactions and real-time payments has widened exposure to phishing, malware, SIM swap fraud, identity theft, account takeover, remote access scams, and fraudulent payment requests. Existing protections are dispersed across the Information Technology Act, RBI circulars, cybersecurity advisories, and payment security rules. Although these measures create a defensive framework, they are often not designed for the speed and complexity of modern FinTech threats. Fraud now frequently exploits user behavior, app design, telecom loopholes, and third-party integrations, while enforcement remains slow and reactive.

Liability in unauthorized transactions is also increasingly difficult to determine. In digital systems, responsibility may involve not only the customer and the bank, but also the payment gateway, telecom operator, wallet provider, app developer, and third-party FinTech platform. RBI guidelines on customer liability offer some operational direction, but statutory ambiguity persists, especially in cases involving manipulation, coercion, or platform weakness rather than direct negligence. Digital lending adds yet another layer of concern. While app-based lending has expanded credit access, especially for underserved populations, it has also been associated with predatory pricing, opaque contractual terms, coercive recovery practices, unauthorized data access, and digital harassment. These developments show that when innovation is weakly supervised, financial inclusion can quickly become a source of consumer vulnerability rather than empowerment.

5. Judicial Developments Shaping E-Banking Regulation

Judicial decisions provide an essential doctrinal foundation for understanding how FinTech and e-banking should be regulated in India, particularly in areas where statutory law remains incomplete or technologically outdated. In the absence of a single, comprehensive FinTech code, courts have helped shape the legal principles

governing privacy, regulatory proportionality, evidentiary standards, and banking liability. These decisions are especially significant because digital finance operates through complex technological systems that frequently raise constitutional, procedural, and accountability questions beyond the scope of traditional banking legislation. As a result, judicial interpretation has become a critical source of normative guidance for the evolving relationship between innovation and regulation in Indian financial law.

A major constitutional foundation for digital financial regulation was laid in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where the Supreme Court affirmed that privacy is a fundamental right under the Constitution of India. This judgment is highly relevant to e-banking because digital financial platforms routinely collect and process highly sensitive personal data, including transaction histories, identity credentials, and behavioral patterns. The case therefore reinforces the idea that data protection in digital banking is not merely a matter of good governance or regulatory convenience, but one of constitutional significance. In the context of FinTech, *Puttaswamy* strengthens the argument for stronger consent norms, data minimization, and safeguards against intrusive financial surveillance.

Equally important is *Internet and Mobile Association of India v. Reserve Bank of India*, in which the Supreme Court examined the legality of the RBI's circular restricting regulated entities from dealing with virtual currency businesses. The Court emphasized that regulatory measures affecting innovation must satisfy the test of proportionality. Although the case arose in the context of virtual currencies, its broader significance lies in clarifying that the RBI has wide regulatory authority, but that such authority must be exercised in a reasoned and proportionate manner. For FinTech regulation more generally, this case highlights the need to balance financial stability and consumer protection with the legitimate space for innovation.

The law relating to electronic evidence has also been clarified through *Anvar P.V. v. P.K. Basheer* and reaffirmed in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*. These decisions are particularly important in digital banking disputes because evidence often consists of electronic records such as transaction logs, app screenshots, text messages, server records, and emails. The Supreme Court in these cases underscored the importance of compliance with Section 65B of the Indian Evidence Act for the admissibility of electronic evidence. This has major implications for FinTech litigation, fraud complaints, and consumer disputes, where the ability to prove digital transactions is often central to the outcome.

Finally, *State Bank of India v. Shyama Devi* remains relevant for foundational principles of banking liability. Although decided in a pre-digital context, the case helps explain when a bank may be held vicariously liable for acts connected to its employees and operational processes. In modern FinTech systems, where transactions involve multiple intermediaries and outsourced digital infrastructures, the case serves as a useful starting point for thinking about accountability in increasingly complex financial ecosystems.

6. Digital Fraud in India: Empirical Trends and Case Studies

The rapid expansion of digital banking has been accompanied by a significant rise in financial fraud, revealing structural weaknesses in the legal framework.

The rapid expansion of digital banking in India has been accompanied by a sharp and measurable rise in financial fraud, revealing deep structural weaknesses in the legal and regulatory framework governing e-banking and FinTech systems. The scale of the problem is evident from recent figures: India recorded approximately 36 lakh cyber fraud cases in 2024, with reported losses exceeding ₹22,800 crore, highlighting the magnitude and systemic nature of the issue . These numbers demonstrate that digital fraud is no longer an isolated phenomenon

affecting a limited number of users; rather, it has become an inherent risk embedded within the rapidly expanding digital financial ecosystem.

A significant contributor to this trend is the increasing reliance on real-time payment systems such as UPI. While these platforms have revolutionized financial transactions by enabling instant, low-cost transfers, they have also created new vulnerabilities. The sharp rise in UPI-related fraud underscores how innovation has outpaced legal safeguards, particularly because transactions occur instantly and are often difficult to reverse . This creates a structural imbalance where technological efficiency exceeds the capacity of legal and institutional response mechanisms.

The nature of fraud itself has evolved significantly. Modern digital fraud is no longer limited to traditional unauthorized access but is increasingly driven by social engineering techniques, including phishing, impersonation, and deceptive communication strategies. Fraudsters manipulate users into voluntarily sharing sensitive information such as OTPs or authorizing transactions under false pretenses. In addition, remote device access and malware attacks allow criminals to gain control over a victim's device, raising complex questions about the extent of user responsibility versus institutional accountability. Similarly, identity theft and KYC misuse expose weaknesses in digital onboarding processes, while the exploitation of UPI platforms through fake requests and malicious links highlights vulnerabilities in system design and consumer awareness .

Case studies further illustrate the seriousness of these issues. In one instance, a digital arrest scam led to a loss of approximately ₹3 crore by a senior citizen in Kolkata, where fraudsters impersonated law enforcement officials and coerced the victim into transferring funds . Such cases challenge traditional legal assumptions about consent, as transactions appear authorized but are in fact the result of psychological coercion. Similarly, phishing and remote access fraud cases, such as those reported in Pune, demonstrate how multiple actors—including banks, telecom providers, and third-party applications—may be involved, making liability determination highly complex. UPI-based instant fraud further compounds the problem, as funds are transferred irreversibly within seconds, while legal remedies remain slow and reactive.

These developments reveal several structural legal issues. First, there is a clear ecosystem liability gap, as existing laws are primarily designed around bank-customer relationships rather than multi-actor digital networks. Second, consent frameworks are outdated, failing to account for manipulation and coercion in digital environments. Third, there is a pronounced mismatch between transaction speed and legal response, with fraud occurring in real time but remedies taking days or weeks. Finally, the complexity of digital evidence, including logs, screenshots, and device data, underscores the importance of evidentiary standards such as those established in *Anvar P.V. v. P.K. Basheer*.

Taken together, these trends demonstrate that digital financial fraud in India is not merely a technological issue but a systemic legal challenge, requiring a shift toward integrated, anticipatory, and ecosystem-based regulation.

7. RBI's Regulatory Response

The Reserve Bank of India (RBI) has taken several significant steps in recent years to regulate the rapidly evolving FinTech ecosystem and strengthen the framework governing e-banking in India. Among its most notable initiatives is the introduction of the regulatory sandbox, which allows FinTech firms to test innovative financial products and services in a controlled environment under regulatory supervision (Reserve Bank of India [RBI], 2019). This mechanism is designed to encourage innovation while minimizing systemic risk, enabling regulators to understand emerging technologies before they are deployed at scale. In addition, the RBI has issued guidelines on digital lending (2022), which seek to regulate lending service providers, enhance

transparency in loan terms, restrict unauthorized data access, and ensure that credit is disbursed and serviced through regulated banking channels (RBI, 2022). These measures reflect a growing recognition of the need to adapt regulatory practices to the realities of digital finance.

While these initiatives represent important progress, they remain largely reactive in nature, responding to issues after they have already emerged rather than anticipating them in advance. For instance, the digital lending guidelines were introduced only after widespread concerns regarding predatory practices, harassment by recovery agents, and misuse of borrower data had surfaced. Similarly, regulatory interventions in areas such as payment security, tokenization, and customer liability have often followed the occurrence of fraud incidents or systemic vulnerabilities. This reactive approach limits the effectiveness of regulation in a FinTech environment characterized by rapid innovation and constantly evolving risk profiles (Arner et al., 2016).

Another limitation lies in the fragmented nature of regulatory instruments, which are often issued in the form of circulars, notifications, or guidelines rather than comprehensive statutory reforms. While such instruments provide flexibility, they may lack the enforceability and coherence of a unified legal framework. Furthermore, the sandbox model, although valuable for experimentation, operates on a limited scale and does not fully address the broader systemic risks associated with large-scale deployment of FinTech solutions.

Consequently, there is an increasing need for the RBI to transition from a reactive, issue-specific approach to a more anticipatory and integrated regulatory strategy. Such a framework would involve forward-looking risk assessment, real-time monitoring mechanisms, clearer allocation of liability, and closer coordination with other regulatory bodies. Only through such a proactive approach can regulation keep pace with innovation and ensure both financial stability and consumer protection in India's evolving digital banking ecosystem.

8. Comparative Perspective

Global regulatory frameworks provide useful benchmarks for understanding how FinTech and e-banking can be governed in a more coherent and forward-looking manner. The European Union's Revised Payment Services Directive (PSD2) is a prominent example of an integrated regulatory approach that promotes both innovation and consumer protection. PSD2 mandates open banking, requiring banks to securely share customer data (with consent) with licensed third-party providers through standardized APIs. This has fostered competition, improved service innovation, and enhanced transparency, while maintaining strong safeguards related to authentication, data protection, and liability (European Commission, 2015). By clearly defining roles and responsibilities within the financial ecosystem, PSD2 reduces ambiguity and strengthens accountability across stakeholders.

Similarly, the United Kingdom's regulatory sandbox, implemented by the Financial Conduct Authority (FCA), represents a proactive approach to FinTech regulation. It allows firms to test innovative financial products under regulatory supervision before full-scale deployment, enabling both innovation and early risk identification (FCA, 2016). Unlike reactive frameworks, the UK model emphasizes continuous regulatory engagement, iterative learning, and collaboration between regulators and innovators.

In contrast, India's regulatory framework remains fragmented and largely reactive, with multiple authorities issuing sector-specific guidelines without a unified legislative structure. While initiatives such as RBI's sandbox and digital lending guidelines reflect progress, they lack the systemic integration seen in global models. Consequently, India faces challenges in ensuring consistent enforcement, clear liability allocation, and comprehensive data governance. Adopting elements of these global frameworks—such as open banking standards and coordinated regulatory mechanisms—could significantly strengthen India's ability to balance innovation with financial stability and consumer protection.

9. Future of E-Banking Laws in India

To effectively address the emerging challenges in the FinTech and e-banking ecosystem, India must transition toward a more coherent, forward-looking, and technology-sensitive regulatory framework. A key priority is the development of a unified FinTech regulatory architecture, which reduces fragmentation and ensures coordination among regulators such as the RBI, SEBI, and MeitY. This would provide clarity for both institutions and consumers operating within hybrid financial systems.

Equally important is the establishment of clear liability frameworks that define responsibility across all stakeholders involved in digital transactions, including banks, FinTech platforms, payment intermediaries, and telecom networks. In the absence of such clarity, consumers remain vulnerable in cases of fraud or system failure. Strengthening data protection laws, particularly in line with constitutional privacy principles recognized in *Puttaswamy v. Union of India* (2017), is essential to safeguard sensitive financial information and ensure trust in digital systems.

Further, the rise of algorithm-driven finance necessitates regulation of artificial intelligence, especially in areas such as credit scoring and risk assessment, to address concerns of bias, opacity, and accountability. The implementation of real-time fraud response mechanisms, including instant transaction freezing and coordinated inter-bank systems, is critical in an environment where fraud occurs within seconds. Finally, adopting an open banking architecture, similar to global models, can promote innovation, competition, and secure data sharing while maintaining strong regulatory oversight.

10. Conclusion

The FinTech revolution has transformed India's financial landscape, but it has also exposed critical gaps in the legal framework governing e-banking. The rise of digital fraud underscores the inadequacy of existing laws, which remain reactive and fragmented. To ensure sustainable growth, India must adopt an anticipatory, ecosystem-based regulatory approach that balances innovation with consumer protection and systemic stability.

References

[1] Arner, D. W., Barberis, J. N., & Buckley, R. P. (2016). The evolution of FinTech: A new post-crisis paradigm. *Georgetown Journal of International Law, 47*(4), 1271–1319.
[2] Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics, 87*(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x
[3] Government of India. (2000). *The Information Technology Act, 2000* (Act No. 21 of 2000). Government of India.
[4] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[5] Reserve Bank of India. (2007). *The Payment and Settlement Systems Act, 2007* (Act No. 51 of 2007). Reserve Bank of India.
[6] Arner, D. W., Barberis, J. N., & Buckley, R. P. (2016). The evolution of FinTech: A new post-crisis paradigm. *Georgetown Journal of International Law, 47*(4), 1271–1319.
[7] Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics, 87*(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x

[8] Reserve Bank of India. (2017). *Customer protection-Limiting liability of customers in unauthorized electronic banking transactions.*
[9] Reserve Bank of India. (2022). *Guidelines on digital lending.*
[10] *Anvar P. V. v. P. K. Basheer*, (2014) 10 SCC 473.
[11] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[12] *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274.
[13] *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[14] *State Bank of India v. Shyama Devi*, (1978) 3 SCC 399.
[15] Government of India. (2023). *Digital Personal Data Protection Act, 2023.*
[16] Reserve Bank of India. (2017). *Customer protection circular.*
[17] Reserve Bank of India. (2019). *Regulatory sandbox framework.*
[18] Reserve Bank of India. (2022). *Digital lending guidelines.*