INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

REGULATION OF DIGITAL BANKING AND FINTECH IN INDIA

AUTHORED BY - DR. RAJEEV KUMAR SINGH
Assistant Professor of Law (Selection Grade)
Amity Law School Lucknow
Amity University Uttar Pradesh, Lucknow Campus

CO-AUTHOR - MS. ASHTA SIDDHI NAGAR
LL.M.
Amity Law School Lucknow
Amity University Uttar Pradesh, Lucknow Campus

Abstract

Global financial services have been transformed by fintech, with an anticipated $24 trillion in transactions in FY21–2022[1]. India has become a major fintech hotspot, with over 7,000 start-ups and a 2021 fintech adoption rate of 87%, which is greater than the global average[2]. It is anticipated that the industry would be valued at $1 trillion by 2030, driven by important industries such as wealth management, digital payments, lending8, and insurance technology. But regulation is still dispersed throughout organisations such as the RBI, IRDAI, SEBI, MCA, and MEITY, which makes it difficult for startups to comply. It is difficult to effectively balance the goals of innovation and consumer protection due to the complicated regulatory environment and the absence of comprehensive fintech laws. The domains, regulators, and tools used in India's fintech rules are examined in this article. It evaluates regulatory strategies for important subsets such as lending structures and digital payments[3]. Pressure points are also highlighted in the analysis, as demonstrated by case studies such as the Paytm debate. In the end, the study makes suggestions for policy optimisation, encouraging fintech development while protecting user interests through careful regulation that is tailored to specific models and risk-aware.

[1] Boston Consulting Group & FICCI, *India FinTech: A USD 1 Trillion Opportunity* (Mar. 2022), https://www.bcg.com/publications/2022/india-fintech-a-usd-1-trillion-opportunity.
[2] EY, *Global FinTech Adoption Index 2019*, EY (June 2019), https://www.ey.com/en_gl/financial-services/ey-global-fintech-adoption-index.
[3] Douglas W. Arner, Janos Barberis & Ross P. Buckley, *The Evolution of Fintech: A New Post-Crisis Paradigm*?, 47 GEO. J. INT'L L. 1271, 1275 (2016).

ISSN: 2582-6433

Keywords – Fintech, Digital Banking, India, Regulation

I. INTRODUCTION

India has one of the fastest growing fintech ecosystem globally, with more than 2,000 recognised fintech enterprises operating across loan, digital payments (P2C and P2P), investment, personal finance, credit ratings, insurance and regulatory technology. The sector is projected to exceed USD 150 billion in value by 2025. In the previous financial year, Indian fintech companies raised approximately USD 8.53 billion through 278 funding deals. Digital payment have shown remarkable growth, with over 23 billion transactions amounting to INR 38.3 lakh crore (around USD 475 billion) recorded by the end of the last financial year's final quarter. Digital payment are expected to dominate overall transaction by 2026, though such projection must be treated cautiously due to potential overestimation.

The sector is largely driven by domestic companies supported by international investment, although foreign players have increasingly entered the Indian market in recent years. The growth is expected to continue particularly in payment supported by expanding internet penetration and favourable policy development. Despite initial disruptions caused by the COVID-19 pandemic, the fintech industry maintained strong momentum. The Governor of the Reserve Bank of India observed that increased digitisation and financial inclusion during the pandemic significantly accelerated fintech adoption. However, as normalcy return, the long-term impact of pandemic-driven digital reliance remain to be assessed. The risk such as a potential global recession and geopolitical instability may also affect sectoral growth.

The key growth area include Buy Now, Pay Later (BNPL), micro-credit, blockchain, open banking, collaboration between fintech firms and traditional banks, neo-banking, embedded finance, artificial intelligence and emerging digital innovation. Embedded finance and "TechFin" models are gaining particular prominence. While projections suggest the sector could reach USD 1 trillion in Assets Under Management and USD 200 billion in revenue, such estimates should be approached with caution due to possible industry optimism.

1.1 Objectives of the study

The present study examine the constitutional and statutory framework governing digital banking and fintech regulation in India. The analysis refers to the Reserve Bank of India Act, 1934 enacted in 1934 which establish the central banking system. It also consider the Payment

ISSN: 2582-6433

and Settlement Systems Act, 2007 enacted in 2007 regulating payment mechanism and settlement procedures. The study includes the Companies Act, 2013 enacted in 2013 that governs incorporation and corporate compliance. Further, the Consumer Protection Act, 2019 enacted in 2019 protect consumer rights in electronic transactions. The Information Technology Act, 2000 enacted in 2000 recognise electronic records and penalise cyber offences. The Digital Personal Data Protection Act, 2023 enacted in 2023 impose statutory obligations concerning personal data processing.

The study analyse regulatory jurisdiction exercised by the Reserve Bank of India, the Securities and Exchange Board of India, the Insurance Regulatory and Development Authority of India and the Ministry of Electronics and Information Technology. It examines how these authorities supervise fintech entities and how their powers intersect within statutory limits. The objectives further include evaluation of consumer protection safeguards in digital finance. The inquiry focus on grievance redressal, unfair trade practice and product liability in online banking disputes. The study also examine the right to privacy affirmed in *Justice K.S. Puttaswamy v. Union of India* decided in 2017 under Article 21 of the Constitution. The obligations under the Digital Personal Data Protection Act, 2023 are analysed in banking context.

The assessment also address regulatory challenges emerging from BNPL, embedded finance, artificial intelligence based lending and cross border payment systems. The issue of regulatory fragmentation and compliance burden under multi agency supervision is examined. The final objective propose structured legal recommendations for balancing innovation with financial stability and consumer protection.

1.2 Research methodology

The present research adopt a doctrinal method based on analysis of statutory enactments, delegated legislation and judicial precedents relating to fintech regulation in India. The primary materials include parliamentary statutes, regulatory circulars, master directions and official notifications. The judicial interpretations provide authoritative exposition of statutory provisions.

The secondary sources consist of academic writings, banking law commentaries and fintech industry reports. The doctrinal analysis interpret provisions in their textual and contextual meaning. The study examine how the regulatory framework balance innovation and prudential

ISSN: 2582-6433

supervision. This method ensure clarity in identifying institutional competence and statutory duties within constitutional structure.

1.3 Review of literature

The existing scholarship discuss fintech governance from perspective of inclusion and regulatory oversight. Reports issued by the Reserve Bank of India analyse digital payments expansion and regulatory sandbox introduced in 2019. These documents emphasise risk based supervision and systemic stability.

Arner, Barberis and Buckley in 2017 examine global regulatory innovation in financial technology. Zetzsche and others in 2018 analyse fragmentation arising from multi regulator supervision. Their study highlight compliance complexities in functional regulatory models./ Policy papers issued by NITI Aayog discuss digital public infrastructure such as Aadhaar and UPI. These papers examine financial inclusion and responsible data governance. Scholarly writings on the Digital Personal Data Protection Act, 2023 analyse consent, breach reporting and cross border data transfer.

The cumulative literature recognise fintech as transformative for financial sector while identifying enforcement gaps and consumer vulnerability in digital ecosystem.

1.4 Research gaps

The literature address fintech expansion and regulatory structure. However integrated doctrinal analysis connecting supervision, consumer protection and data privacy remain limited. The fragmentation among RBI, SEBI, IRDAI and MeitY receive acknowledgment yet it legal consequences on compliance burden lack detailed study. Emerging fintech model receive limited prudential scrutiny. The implementation challenge of the Digital Personal Data Protection Act, 2023 in banking sector remain insufficiently examined.

The comparative alignment of Indian framework with international standards on cross border data governance require structured legal analysis. The debate between innovation oriented regulation and strict supervisory control continue without comprehensive doctrinal articulation within Indian socio economic context.

ISSN: 2582-6433

1.5 Research Question

- How the fragmented regulatory framework in India among RBI, SEBI, IRDAI and MeitY impact fintech growth, innovation, and the protection of the consumer? The overlapping jurisdiction sometime create confusion and increase the compliance burden. The coordination between these authorities also delay dispute resolution and supervision of emerging financial models.
- How the existing laws like Payment and Settlement Systems Act, 2007, Companies Act, 2013, Consumer Protection Act, 2019 and the Digital Personal Data Protection Act, 2023 address fintech model such as BNPL, AI lending and embedded finance? The clarity of duties and enforcement remain uneven and sometimes conflicting.
- How the measures including regulatory sandbox launched by RBI in 2019, inter-agency coordination and data protection compliance strengthen innovation and supervision in fintech? The procedural burden remain high and the alignment with global regulatory standard stay limited for cross-border operations.

II. THE KEY LAWS AND REGULATIONS GOVERNING THE FINTECH SECTOR IN INDIA

FinTech is an abbreviation for financial technology, covering any technology used to facilitate financial transactions or services, provided by any business. FinTech, in commercial and regulatory terms, refers to the technology employed by financial service providers to change the conventional method of delivering services. businesses like Paytm, PhonePe, RazorPay, MobiKwik, and PayU are categorised as fintech enterprises.[4]The fintech business in India has experienced significant innovation and expansion in recent years, driven by the expanding internet and smartphone use. Fintech firms provide technology-driven financial services such as digital payments, online lending, wealth management, and insurance aggregation. Regulating a dynamic business demands examination to reconcile innovation with financial stability and customer safety. The regulatory framework for Indian fintech is divided among many authorities including the "Reserve Bank of India" (RBI)[5], "Securities Exchange Board of India" (SEBI), "Insurance Regulatory and Development Authority of India" (IRDAI), and

[4] Invest India, *Fintech Industry in India*, *INVEST INDIA* (2023), https://www.investindia.gov.in/sector/bfsi-fintech-financial-services.
[5] Reserve Bank of India, *Report of the Working Group on Digital Lending Including Lending Through Online Platforms and Mobile Apps* (Nov. 18, 2021), https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1215.

ISSN: 2582-6433

"Ministry of Electronics and Information Technology" (MeitY). Fintech goods and services are subject to regulations relevant to the industry, although further progress is needed in areas such as data protection and consumer complaint resolution.

2.1 Payment Fintechs

Entities providing digital payment services must get approval from the RBI under the "Payments and Settlement Systems" (PSS) Act 2007 before starting operations. The PSS Act regulates many payment systems such as "prepaid payment instruments" (PPIs), money transfer services, and card networks. Relevant regulations include technology risk management, consumer protection measures, and data security requirements. Securities broking and investment advising operations need licencing under the "SEBI (Stock Brokers) Regulations 1992 and the SEBI[6] (Investment Advisers) Regulations 2013", respectively. Insurance online aggregators, brokers, and agents must be licenced by the IRDAI legislation pertaining to their roles: "Insurance Online Aggregators Regulations 2017, Insurance Brokers Regulations 2018, and Registration of Corporate Agents Regulations 2015.

The Payment and Settlement Services Act of 2007 mandates the Reserve Bank of India (RBI) to grant authorisation to non-bank payment system operators before starting such services. PSOs include payment service providers, card networks, and aggregators of payments. The RBI has issued further regulations, circulars, and directions for these operators, including the Master Directions on Prepaid Payment Instruments 2021[7] and the Guidelines on Regulation of Payment Aggregators and Payment Gateways. Non-bank lending and factoring firms must gain licencing as NBFCs. The "Unified Payments Interface" (UPI) enables clients to link their bank accounts to a single mobile app, simplifying the consolidation of financial services, seamless fund flow, and the ability to pay merchants. The "Bharat Interface for Money" (BHIM) program facilitates quick, secure payments via UPI, allowing direct bank payments by inputting their UPI ID or scanning their QR code.

Infrastructure (NPCI) was created in 1956 as a joint venture between the Reserve Bank of India and the Indian Banks' Association to improve India's retail payment and settlement systems.

[6] Securities and Exchange Board of India (Stock Brokers) Regulations, 1992 (India); *Securities and Exchange Board of India (Investment Advisers) Regulations*, 2013 (India).
[7] Reserve Bank of India, *Guidelines on Regulation of Payment Aggregators and Payment Gateways*, DPSS.CO.PD.No.1810/02.14.008/2019-20 (Issued on Mar. 17, 2020) (India); Reserve Bank of India, Master Direction on Prepaid Payment Instruments (PPI-MD), RBI/DPSS/2021-22/02 (Issued on Aug. 27, 2021) (India).

ISSN: 2582-6433

The primary promoter group includes "State Bank of India, Punjab National Bank, Canara Bank, Bank of Baroda, Union Bank of India Limited, Bank of India Limited, ICICI Bank Limited, HDFC Bank Limited, Citibank N. A., and Hong Kong and Shanghai Banking Corporation."[8] In 2016, 56 member institutions participated in the ownership round. Currently, UPI integration into customer-facing online platforms or mobile applications is limited to banks, although banks and non-banks can collaborate to fuel UPI payments through technology, design, or operation.

2.2 Incorporated Fintechs

Fintech firms, as corporate organisations, are required to adhere to the Companies Act 2013 for KYC standards, record-keeping obligations, and submissions. financial statement.The Companies Act, 2013 provides three major business structures: sole proprietorship, Limited Liability Partnership (LLP), and Private Limited Company (PLC). When creating a business, individuals should analyse these possibilities based on the organization's size, vision, and objective to determine the most effective structure for raising capital and maximising profitability.

Subsequently, they should establish and register the business in compliance with legal regulations. People sometimes question how to register a FinTech of the vast quantity of data they create about consumer payments and transactions. Some of the paperwork necessary during the time of incorporation may include. The firm's ownership of the FinTech's intellectual property is defined in the Partnership Agreement/AOA IPR Licencing Agreement. Protecting Personal Information: The Information Technology Act of 2000 (IT Act) specifies standards for the handling of sensitive data, including financial data, throughout company's GST ID. Obtaining a unique "Goods and Service Tax Identification"[9] (GSTI) is needed for a corporation to comply with the Goods and Service Tax registration requirements. The GSTI, established by a Tax Identification Number (TIN), is vital for tax identification and registration in the indirect taxation system. FinTech enterprises are required to comply with this rule because of the vast amount of data they collect regarding consumer payments and sales.

[8] National Payments Corporation of India, About NPCI, NPCI (Jan. 10, 2024, 11:00 AM), https://www.npci.org.in/who-we-are/about-us.
[9] Goods and Services Tax Network, *GST Registration, GST* (Jan. 12, 2024, 3:10 PM), https://www.gst.gov.in/.

ISSN: 2582-6433

III. CONSUMER PROTECTION

The Consumer Protection Act 2019 forbids unfair trading practices, such as the unauthorised sharing of customers' sensitive data. The Information Technology Rules 2011[10] include prohibitions that ban fintech platforms from sharing users' sensitive personal information without authorization. These limits are aimed to protect consumers' personal and financial information. Before the implementation of the CPA 2019, client safety in online banking was based on several legislation from multiple organisations. The RBI[11] released directives on consumer due diligence, grievance redress, and electronic banking security. Specialised laws such as the IT Act of 2000 and the Banking Regulation Act of 1949 dealt with issues connected to data privacy and electronic transactions. Yet, these policies were uneven and not focused on the requirements of customers, resulting in gaps in protection.

3.1 The Consumer Protection Act 2019: A New Paradigm

The CPA 2019 marks a dramatic shift, enacting a comprehensive framework for consumer protection across all industries, including financial services. Key provisions relevant to internet banking include:[12]

- Enhanced consumer rights: The Act expands consumer rights beyond traditional conceptions of safety and fair pricing. It enshrines rights to information, informed consent, choice, grievance redressal, and compensation for unjust practices.
- Liability for defective services: Banks are now accountable for services failing to fulfil promised standards, particularly in the online sphere. This incentivizes them to invest in secure systems and robust customer service.
- Grievance redressal mechanisms: The Act established a three-tier structure for grievance redressal, culminating in the Central Consumer Protection Authority (CCPA) for unresolved complaints. This provides customers with a more accessible and streamlined forum for seeking redressal. Penalties for violations: Stringent penalties, including jail and hefty fines, prohibit unfair activities and promote responsible conduct by banks.[13]

[10] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 6 (India).
[11] Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, RBI/DPSS/2019-20/174 (Issued on Feb. 18, 2021) (India).
[12] Avtar Singh, *Consumer Protection: Law and Practice* 112 (Eastern Book Company, 3d ed. 2020).
[13] Shailendra Kumar, *Consumer Protection in Banking Services*, 12 NUJS L. REV. 85, 96 (2019).

ISSN: 2582-6433

3.2 Impact and Challenges

The CPA 2019 has ushered in a new age of consumer protection in online banking. Consumers are now empowered with defined rights and options for seeking redressal. The Act has also prompted banks to tighten their compliance measures and security protocols. However, issues remain: Awareness and accessibility: Many consumers, especially in rural regions, are unaware of their rights under the Act or face difficulty accessing the redressal mechanisms. Implementation: Effective implementation of the Act rests on the CCPA's capacity and consumer forums' effectiveness. Technology-driven challenges: Emerging technologies like artificial intelligence and big data bring new risks security, needing to privacy and continuous adaptation of the regulatory framework.

3.3 Major modifications in the definition of "consumer" under the Consumer Protection Act, 2019 are as following;

- Online buyers.
- The 2019 Act also includes the endorsement of products and services, often done out by celebrities.
- Endorsers now have an added responsibility, together with manufacturers and service providers, to avoid erroneous or misleading marketing.
- Unlike the 1986 Act, the definition of "goods" has been updated to include "food" as defined in the Food Safety and Standards Act, 2006. This would also include the fast rising number of food delivery platforms under the 2019 Act.

The word of "services" in the 2019 Act has been amended to include "telecom" in order to include telecom service providers. However, it is interesting that this inclusion has not been officially classified as "telecommunication service" as defined in the Telecom Regulatory Authority of India Act, which typically include internet, cellular, and data services. The 2019 Act includes a prominent provision called "product liability," which holds manufacturers and sellers accountable for paying consumers for any damage caused by faulty goods or services. Another recently adopted idea is "unfair contracts," designed to defend customers from one-sided and irrational agreements that heavily benefit manufacturers or service providers.[14]

[14] G. Ramesh Kumar, *Consumer Protection Act, 2019: A Critical Analysis*, 11 INDIAN J. L. & JUST. 45, 58 (2020).

ISSN: 2582-6433

The definition of "unfair trade practices" now encompasses misleading electronic advertising, failure to accept returns of faulty goods or inadequate services, and failing to provide a refund within the designated time period or within thirty days if no time frame is indicated. It is now considered a felony to expose any personal information that was submitted in confidence and gathered during a transaction.[15]

IV. DATA PRIVACY

The IT Act of 2000, coupled with its "Reasonable Security Practices and Sensitive Personal Data Rules," largely control data privacy in the fintech sector at present. Despite being insufficient for the business, they need security measures and consent restrictions for the gathering and use of personal data by fintech platforms. More stricter data protection measures are envisaged. The Indian Constitution does not specifically guarantee the fundamental right to privacy. Courts have regarded the right to privacy as a essential part of other fundamental rights including freedom of speech and expression under "Article 19(1)(a) and the right to life and personal liberty under Article 21 of the Indian Constitution." The Fundamental Rights in the Constitution of India are subject to reasonable limits as outlined in Article 19(2) that could be imposed by the State. In the decision of "Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors.,[16]" the constitution bench of the Supreme Court established the Right to Privacy as a fundamental right, subject to limited permitted restrictions.[17]

The Indian Information Technology Act of 2000 categorises hacking as a serious offence under Section 66. Hacking is generally acknowledged as a criminal act connected to compromising knowledge security. The competent government (central/state) has the authority to designate any 'computer', 'computer system', or 'computer network' as a protected system. Someone who gains access to the 'protected computer system' against the law can face a 10-year prison sentence and a large fine[18].

The Information Technology Act, of 2000, sometimes known as the "IT Act," attempts to legally recognise transactions made by electronic data interchange and electronic communication, commonly known as "electronic commerce."

[15] P. K. Majumdar, *Consumer Protection in the Era of E-Commerce*, 62 J. INDIAN L. INST. 327, 340 (2020).
[16] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[17] M. P. Jain, *Indian Constitutional Law* 1365–1372 (8th ed. 2018).
[18] S. Bhattacharjee, *Cyber Crime and the Indian Information Technology Act: An Analysis*, 8 INDIAN J.L. & TECH. 56, 63 (2012).

ISSN: 2582-6433

This involves using electronic means instead of paper-based ones to transmit and store information, enabling electronic filing of documents with government bodies.Indian banks are expected to comply with data privacy requirements contained in the "Information Technology Act, of 2000, the Prevention of Money Laundering Act, of 2002, and guidelines from the Reserve Bank of India (RBI). Once the Digital Personal Data Protection Act, 2023 (DPDP Act)" is implemented and its regulations (DPDP Rules) are released, banks and other financial institutions will undergo a significant change in their data processing procedures.[19]

4.1 Implications for Indian banks for the application of these laws are important and multifaceted:

- Consent for Data Processing: Banks must personally tell both existing and new clients about data processing. Consent is triggered not just by account based connections but also by any processing of identifiable personal data. This comprises diverse services such visitor information processing, risk management, and product development. Data sharing inside a bank's group is permissible with specific consent for the intended objectives.[20]
- Outsourcing to Data Processors: Banks bear primary obligation as Data .Fiduciaries for personal data processing by intermediaries such as KYC verification agents and payment system providers. Responsibility extends to sub-agents under the DPDP Act, albeit joint liability requirements are not yet created.[21]
- Data Breach Reporting: Immediate reporting of personal data breaches to both impacted customers and the Data Protection Board is mandatory under the DPDP Act. Failure to comply can lead to significant penalties.[22]
- Internal Policies: Grievance redressal methods need to explicitly handle personal data complaints. Special policies for items involving children's data are necessary. A separate system should be established for managing data rectification and erasure requests.[23]

[19] Pavan Duggal, *Cyberlaw & Data Protection in India* 312–320 (2nd ed. 2022).
[20] Tal Z. Zarsky, Incompatible: *The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1012 (2017).
[21] Ira S. Rubinstein, Big Data: *The End of Privacy or a New Beginning*?, 3 INT'L DATA PRIV. L. 74, 89 (2013).
[22] Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 112–118 (2018).
[23] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023: Overview and Compliance Framework, MeitY* (Aug. 15, 2023, 10:00 AM), https://www.meity.gov.in.

ISSN: 2582-6433

- Cross-Border Data Transfer: Transfer of customer data outside India for specified purposes requires consent and compliance with DPDP Act standards.[24]
- Co-Branding Arrangements: Indian banks are regarded Data Fiduciaries, and card issuers are called Data Processors in co-branding arrangements. Compliance with both the DPDP Act and RBI directives is necessary.
- Use of AI: Banks using AI, such as big language models, must guarantee sufficient consent for personal data use unless the data is public or voluntarily submitted for AI purposes.

These implications need substantial policy adjustments and procedural changes within Indian banks to achieve compliance with the DPDP Act and related regulations.

V. RBI REGULATIONS

Fintech lenders must acquire authorisation from the RBI to begin operations as NBFCs, while also satisfying eligibility standards linked to capital sufficiency and risk management expertise. RBI laws supervise lending rates, customer grievance redressal processes, and adherence to the fair practices code. The RBI oversees new specialised banks including small financing banks and payment banks, imposing customised capital and coverage standards to promote financial inclusion. Payment intermediates are businesses that accept funds from customers for online transactions and then transfer the money to the merchants as payment for the goods or services acquired by the customers. Payment intermediates do not accommodate transactions that are comparable to a delivery versus payment arrangement. In November 2009[25], the RBI released the 2009 EPT Directions under section 18 of the P&SS Act. These directives were put in place to preserve customers' interests and make sure that intermediaries account for their payments appropriately and get them to merchants quickly.[26]

The 2009 EPT Directions describe intermediaries as businesses that collect payments from clients via electronic or online means and transfer these sums to merchants. Financial institutions are forbidden from establishing or operating accounts for collecting payments from

[24] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023: Overview, MeitY* (Aug. 15, 2023, 10:00 AM), https://www.meity.gov.in.
[25] Reserve Bank of India, *Directions for Opening and Operation of Accounts and Settlement of Payments for Electronic Payment Transactions Involving Intermediaries,* DPSS.CO.No.619/02.14.008/2009-10 (Issued on Nov. 24, 2009) (India).
[26] Reserve Bank of India, *Guidelines on Regulation of Payment Aggregators and Payment Gateways, DPSS*.CO.PD No.1810/02.14.008/2019-20 (Issued on Mar. 17, 2020) (India).

ISSN: 2582-6433

merchants' clients via intermediaries, which must be recognised as internal bank accounts. These accounts must be audited and certified by Transfers the RBI every quarter from other banks into the intermediary's primary bank account, credits for payments made by multiple parties for the purchase of goods or services, and transfers returned for failed or disputed transactions are allowed under the 2009 EPT Directions. The intermediary's principal bank account may be debited for merchant and service provider payments, transfers to other banks according to a pre-arranged arrangement, refunds for disputed or failed transactions, commissions at particular rates. The RBI announced the Payment Aggregators and Payment Gateways Guidelines on March 17, 2020, and will be in effect starting April 1, 2020[27]. Payment Gateways provide the essential technical infrastructure for online payment transactions, while Payment Aggregators connect merchants and acquirers. Current PAs must have a net worth of Rs. 15,00,00,000 by March 31, 2021, and Rs. Prospective PAs must have a net worth of at least Rs. 15,00,00,000 before obtaining permission, and their net worth must climb to Rs. 25,00,00,000 by the end of the third fiscal authorization year after gaining.

All accepted payments must be held in an escrow account with a scheduled commercial bank by non-bank payment aggregators (PAs). They can only keep the money in one bank at a time. When payments can be made to merchants and how much can be deposited into the escrow account are both outlined in the PAPG Guidelines. After the merchant confirms delivery, notifies the intermediary of the cargo, or if the merchant chooses otherwise, PAs must pay the merchant within a day. The escrow account can be pre-funded by PAs using their own funds or the merchant's funds, and the merchant will have a beneficial stake in the pre-funded sum.
The 2009 EPT Directions exempt intermediates, such as non-bank PAs and PGs, from obtaining an RBI licence. PAs must, however, be Indian businesses that were founded in accordance with the Companies Act of 1956 or 2013**.**

VI. INSURANCE AGGREGATORS

InsurTech businesses that let customers shop, compare, and purchase insurance online are required to hold an IRDAI insurance broker or corporate agent licence. Direct distribution and sales of insurance goods to retail clients are now simpler thanks to recent partnerships between fintech platforms and insurers. InsurTech is the use of technology to deliver a cutting-edge insurance service. Important InsurTech businesses in India are Digit Insurance, Policy Bazaar,

[27] Reserve Bank of India, *Framework for Regulation of Payment Aggregators, RBI Bulletin* (Apr. 2020), https://www.rbi.org.in.

ISSN: 2582-6433

and Acko. To regulate InsurTech in India, the Indian Insurance Regulatory Authority (IRDAI) has published a number of rules and guidelines. The Insurance Regulatory and Development Authority of India (Issuance of eInsurance Policies) Regulations, 2016;[28] the Guidelines on Insurance e-commerce, dated March 9, 2017; and the Guidelines on insurance repositories and electronic issuance of insurance policies, dated May 29, 2015. [29]

The Guidelines for Repositories and Electronic Policy Issuance govern insurance policy repositories. Insurance policy data can be stored on behalf of insurers by a licensed company that has been approved by IRDA as an Insurance Repository (IR). Insurers must use an IR and sign service-level agreements with at least one IR in order to issue and administer e-insurance policies. Any IR must have a current, three-year-valid registration certificate from IRDA in order to operate. The internal auditor oversees thorough internal monitoring, evaluation, and assessment of controls and systems. Every year, an external system audit firm with IRDA authorisation is required to review the industry's safeguards, systems, procedures, and controls. Policyholders, nominees, assignees, beneficiaries, and endorsements in electronically issued policies are all listed in the Insurance Regulator's records of electronic insurance accounts. Every record is given a distinct number along with the assignment date. A variety of insurance policies, including life and general insurance plans, will be stored electronically by the IR. Subject to specific yearly premiums and insured levels, the e-insurance Policies Regulations require issuers to offer policyholders electronic insurance policies. Different laws govern various insurance policy types, including individual health, pensions, pure term, and non-pure term. Policyholders must have an electronic insurance account, and insurance policies can be offered directly or through agents. In certain situations, insurers are required to offer tangible insurance. The procedure for providing electronic insurance policies is described in the e-insurance Policies Regulations. With a code of conduct and steps for setting up an ISNP to participate in insurance e-commerce in India, the Insurance e-Commerce Guidelines permit the establishment of Insurance Self-Network Platforms (ISNPs) for the administration and sale of insurance policies.[30]

In order to supervise and regulate web aggregators as insurance intermediaries that run websites that enable insurance prospects to compare rates and access product information from multiple

[28] K. C. Mishra & G. E. Thomas, *General Insurance: Principles and Practice* 412 (Cengage Learning India, 2d ed. 2017).
[29] R. Srinivasan, *InsurTech: A Legal and Regulatory Perspective in India*, 12 J. INS. INST. INDIA 45, 52 (2020).
[30] P. K. Gupta, *Insurance and Risk Management 389 (Himalaya Publishing House*, 4th ed. 2018).

ISSN: 2582-6433

insurers, the IRDA implemented the "Insurance Regulatory and Development Authority of India (Insurance Web Aggregators) Regulations, 2017." To operate, these insurance web aggregators need to obtain a registration certificate from the IRDA. They sell insurance online or by telemarketing, display product comparisons on insurance web aggregator websites, and engage in other marketing initiatives.[31]

VII. SUGGESTION

7.1 Legislation.

The introduction of a unified fintech statute will reduce fragmentation between the Reserve Bank of India, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India and the Ministry of Electronics and Information Technology. The statutory clarity strengthen jurisdictional certainty and accountability.

7.2 Inter regulatory coordination.

The establishment of a formal coordination mechanism between financial and technology regulators ensure supervisory consistency. This structure reduce overlaps and procedural conflict in digital banking oversight.

7.3 Effective consumer protection.

The enforcement under the Consumer Protection Act, 2019 enacted in 2019 require institutional strengthening. The grievance redressal forums need administrative capacity and digital accessibility for consumers.

7.4 Data protection compliance.

The alignment with the Digital Personal Data Protection Act, 2023 enacted in 2023 and the Information Technology Act, 2000 enacted in 2000 impose statutory data obligations. The internal audits and breach reporting mechanism demands uniform standardisation.

7.5 Sandbox and innovation control.

The regulatory sandbox introduced by the Reserve Bank of India in 2019 require expansion for cross sector products. This supervised experimentation maintain prudential discipline and innovation balance.

[31] Sandeep Sharma, *Regulation of Insurance Intermediaries in India*, 9 J. INS. L. & PRAC. 112, 118 (2020).

ISSN: 2582-6433

7.6 Clear norms for emerging models.

The regulatory guidelines for BNPL and AI based lending require specific disclosure and capital standards. The clarity prevent arbitrage and strengthen compliance structure.

7.7 Cybersecurity and compliance simplification.

The uniform cybersecurity protocol for payment aggregators and NBFCs ensure system integrity. The simplified digital licensing portal under the Companies Act, 2013 enacted in 2013 and the Payment and Settlement Systems Act, 2007 enacted in 2007 reduce procedural burden while preserving regulatory supervision.

VIII. CONCLUSION

The expansion of internet access and financial inclusion programmes present a strong foundation for the Indian fintech sector. The industry records significant growth with projected revenue of USD 200 billion and Assets Under Management of USD 1 trillion by 2025. This growth indicate structural transformation in financial service and digital delivery model.

The regulatory framework remains distributed across authorities such as the Reserve Bank of India, Securities and Exchange Board of India and Insurance Regulatory and Development Authority of India. The enforcement of the Consumer Protection Act 2019 enacted in 2019 strengthen consumer right yet implementation gap persist. The data protection obligations under the Digital Personal Data Protection Act, 2023 impose compliance responsibilities on banks and fintech entities. The cybersecurity safeguards and breach reporting mechanisms demand institutional strengthening.

The financial inclusion objective emphasise digital literacy and affordable connectivity for underserved communities. The cooperation between regulators and fintech institutions promote innovation within supervised environment including sandbox initiatives. The international expansion of Indian fintech firm require alignment with global regulatory standard and structured cross border coordination. The collective institutional response remain essential for sustainable fintech governance.

ISSN: 2582-6433

References

- Boston Consulting Group & FICCI, *India FinTech: A USD 1 Trillion Opportunity* (Mar. 2022).
- EY, *Global FinTech Adoption Index 2019*, EY (June 2019).
- Douglas W. Arner, Janos Barberis & Ross P. Buckley, *The Evolution of Fintech: A New Post-Crisis Paradigm?*, 47 GEO. J. INT'L L. 1271 (2016).
- Invest India, *Fintech Industry in India* (2023).
- Reserve Bank of India, *Report of the Working Group on Digital Lending Including Lending Through Online Platforms and Mobile Apps* (Nov. 18, 2021).
- Securities and Exchange Board of India, *Stock Brokers Regulations, 1992* (India)
- Securities and Exchange Board of India, *Investment Advisers Regulations, 2013* (India)
- Reserve Bank of India, *Guidelines on Regulation of Payment Aggregators and Payment Gateways*, DPSS.CO.PD.No.1810/02.14.008/2019-20 (Issued Mar. 17, 2020)
- Reserve Bank of India, *Master Direction on Prepaid Payment Instruments (PPI-MD)*, RBI/DPSS/2021-22/02 (Issued Aug. 27, 2021).
- National Payments Corporation of India, *About NPCI* (Jan. 10, 2024).
- Goods and Services Tax Network, *GST Registration* (Jan. 12, 2024).
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 6 (India)
- Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, RBI/DPSS/2019-20/174 (Issued Feb. 18, 2021)
- Avtar Singh, *Consumer Protection: Law and Practice* 112 (Eastern Book Company, 3d ed. 2020)
- Shailendra Kumar, *Consumer Protection in Banking Services*, 12 NUJS L. REV. 85 (2019)
- G. Ramesh Kumar, *Consumer Protection Act, 2019: A Critical Analysis*, 11 INDIAN J. L. & JUST. 45 (2020)
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India)
- Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023: Overview and Compliance Framework*, MeitY (Aug. 15, 2023).
- Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995 (2017)
- Pavan Duggal, *Cyberlaw & Data Protection in India* 312–320 (2nd ed. 2022)