International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Fintech and the Right to Privacy: Data Protection in Digital Finance

Dr. Vipinkumar M[1], Ms. Akshara B[2]

[1]Assistant Professor, Department of Management Studies, MES AIMAT, Ernakulam, Kerala, India
[2]Assistant Professor in Law, Bharata Mata School Of Legal Studies, Ernakulam, Kerala, India

ABSTRACT

The rapid advancement of financial technology (Fintech) has transformed the landscape of financial services by enabling faster, more inclusive and customer-centric operations. However, the increasing reliance on personal data to power digital finance platforms has raised significant concerns regarding data privacy and individual rights. This paper investigates the relationship between Fintech growth and the right to privacy, examining how financial data is collected, processed, and protected in digital environments. It analyzes the effectiveness of current legal frameworks such as the General Data Protection Regulation (GDPR), India's Digital Personal Data Protection Act, and sector-specific Fintech regulations. The research highlights the tension between innovation and regulation, identifies risks to user's privacy, and evaluates the role of ethical data governance. Based on qualitative content analysis and secondary data review, the study provides insights into user trust, regulatory enforcement, and policy gaps, ultimately recommending stronger compliance measures and digital literacy programs.

Keywords: Fintech, Right to Privacy, Data Protection, Digital Finance, GDPR, Data Governance, Digital Personal Data Protection Act (DPDP), Cyber security, User Trust, Financial Technology.

1. INTRODUCTION

The digital revolution has fundamentally altered financial services, giving rise to Fintech—a sector that merges finance and technology to deliver innovative services such as mobile payments, peer-to-peer lending, digital banking, and robo-advisors. While Fintech has expanded financial inclusion and efficiency, it has also introduced complex data privacy concerns. The vast amount of personal and financial data processed by these platforms makes users vulnerable to breaches, surveillance, and misuse. In democratic societies, the right to privacy is a fundamental human right, enshrined in international covenants and constitutional law, such as Article 21 of the Indian Constitution. As such, the regulation of data protection in Fintech is both a legal and ethical imperative.

The convergence of finance and technology—popularly known as **Fintech**—has fundamentally reshaped the financial services landscape. From mobile banking and digital wallets to peer-to-peer lending, robo-advisors, and blockchain-based platforms, Fintech has disrupted traditional banking by making financial services more accessible, efficient, and user-friendly. These innovations have especially empowered previously unbanked and under banked populations, driving financial inclusion on a global scale.

[1] Assistant Professor , Department of Management Studies , MES AIMAT, Ernakulam , Kerala, India
[2] Assistant Professor in Law , Bharata Mata School Of Legal Studies, Ernakulam , Kerala, India

However, the rapid digitization of financial services is not without significant drawbacks. One of the most critical and contentious issues is **data privacy**. Fintech platforms rely heavily on the collection, analysis, and storage of large volumes of personal, financial, and behavioral data. This data is often used to customize services, assess creditworthiness, detect fraud, and enhance user experience. While these applications offer convenience, they simultaneously pose risks to users' privacy and autonomy.

In this data-driven environment, the right to privacy—long considered a cornerstone of democratic societies and enshrined in various international human rights instruments—faces serious threats. Privacy is not merely about data protection; it encompasses the right of individuals to control information about themselves and to be free from unwarranted surveillance, profiling, and manipulation. With algorithms making decisions that affect credit scores, loan approvals, and even insurance premiums, the implications of data misuse in Fintech can have direct and lasting consequences on people's lives. The situation is further complicated by asymmetric power dynamics between Fintech companies and users. Most consumers lack the knowledge, time, or resources to understand complex privacy policies or challenge the misuse of their data. Consent is often obtained through lengthy, opaque terms of service that users are required to accept in order to access essential financial services. In many cases, this consent is neither fully informed nor freely given, undermining the principles of informed consent and user autonomy.

Recognizing these concerns, governments and regulators around the world have begun implementing legal frameworks aimed at protecting personal data. The **European Union's General Data Protection Regulation (GDPR)** is a global benchmark, mandating transparency, accountability, and user rights. India has followed suit with the enactment of the **Digital Personal Data Protection Act (DPDP) 2023**, signaling a growing recognition of data privacy as a fundamental right. However, the enforcement of these regulations, particularly in the fast-evolving and fragmented Fintech sector, remains a significant challenge.

Moreover, Fintech companies operate across borders, leading to jurisdictional challenges in data protection. While some companies adopt global best practices, many startups, especially in emerging markets, lack the resources or incentives to implement robust data governance frameworks. This creates a fragmented privacy landscape where users' rights vary depending on geography, regulation, and platform maturity.

Given this complex backdrop, this paper seeks to explore the intersection of **Fintech and the right to privacy**, with a focus on how digital finance platforms collect, process, and protect user data. It evaluates the effectiveness of existing legal frameworks, corporate practices, and technological solutions in ensuring data protection. Additionally, it examines the ethical and human rights dimensions of digital finance, advocating for a privacy-first approach that balances innovation with individual rights.

The research is timely and relevant, not only because of the explosive growth of Fintech but also due to the increasing awareness among consumers and policymakers about the importance of data rights. By analyzing the legal, technological, and ethical dimensions of data protection in Fintech, this study aims to contribute to the ongoing discourse on building a safe, inclusive, and rights-respecting digital financial ecosystem. This paper seeks to examine how Fintech intersects with privacy rights and assess whether current frameworks adequately protect users in the digital finance landscape.

2. LITERATURE REVIEW

Fintech, short for financial technology, has disrupted traditional financial systems by leveraging emergi-

ng technologies such as artificial intelligence (AI), big data analytics, blockchain, and mobile platforms to enhance the delivery of financial services. As **Arner, Barberis, and Buckley (2016)** explain, fintech has created new paradigms of service efficiency, access, and customization. However, this innovation comes at the cost of increased data dependency, with fintech platforms requiring vast amounts of personal, behavioral, and financial data to function effectively. **Gai, Qiu, and Sun (2018)** note that this heavy reliance on data exposes users to significant risks concerning the misuse or unauthorized access of sensitive information.

Data privacy has emerged as a crucial concern in the digital finance environment. **Solove (2006)** argues that privacy is multifaceted, encompassing issues such as information collection, processing, dissemination, and invasions. In fintech, these concerns are magnified due to the dynamic and often opaque nature of data processing. **Zetzsche et al. (2017)** highlight that many fintech firms operate in regulatory environments where privacy norms are either underdeveloped or unevenly enforced, creating loopholes for data exploitation. The lack of transparency and informed consent mechanisms exacerbates these risks, leading to potential infringements on users' right to privacy.

The European Union's *General Data Protection Regulation (GDPR)* is widely regarded as a global benchmark in data protection, establishing stringent rules for data processing, consent, data subject rights, and cross-border data transfer (**Voigt & von dem Bussche, 2017**). **Tikkinen-Piri, Rohunen, and Markkula (2018)** emphasize how GDPR has influenced international regulatory practices by promoting user empowerment and accountability.

India has recently enacted the Digital Personal Data Protection (DPDP) Act, 2023, marking a significant shift in its data governance landscape. The Act introduces core principles such as consent-based data processing, purpose limitation, and accountability of data fiduciaries. However, critics like **Sharma (2023)** argue that the law offers broad exemptions for government entities and lacks stringent enforcement provisions, raising concerns about its ability to effectively regulate Fintech entities and protect consumer data.

Fintech business models, particularly in lending, insurance, and financial advisory services, depend on alternative data sources like smartphone usage, geolocation, and social media activity. While such data usage can expand access to financial services and enhance credit assessments **(Bazarbash, 2019)**, it also raises ethical and privacy concerns. Algorithmic profiling, lack of informed consent, and the potential for discrimination are key risks associated with this model.

Narayanan and Vallor (2019) stress that the "black-box" nature of many AI-driven systems used in fintech makes it difficult for users to understand how decisions affecting them are made. This lack of transparency and accountability leads to a power imbalance, where consumers are unable to challenge or question automated decisions that may adversely affect them.

Trust in data protection practices significantly influences consumer adoption and sustained use of Fintech services. **Lee and Shin (2018)** report that concerns over privacy and security are central to user decisions regarding Fintech engagement. Similarly, Liébana-Cabanillas, **Marinkovic, and Kalinic (2017)** highlight that perceived control over personal data and institutional trust are strong predictors of user loyalty.

However, the phenomenon known as the "privacy paradox" persists—despite expressing concerns about data privacy, many users continue to share personal information due to convenience or lack of understanding of privacy implications. This points to a need for greater digital literacy and transparency in data usage. Recent research has explored the role of privacy-enhancing technologies in mitigating

risks. Block chain, with its decentralized architecture, is seen as a tool to enhance security and reduce centralized data vulnerabilities **(Xu, Chen, & Kou, 2019)**. Other technologies such as homomorphic encryption, differential privacy, and zero-knowledge proofs are gaining traction for enabling data analysis without exposing individual-level data.

Nonetheless, Radanliev et al. (2020) argue that despite their promise, these technologies face barriers in scalability, usability, and regulatory clarity. Fintech firms may find it challenging to integrate such tools into their existing systems due to cost, complexity, and lack of standardization. Beyond legal frameworks, the ethical implications of data practices in fintech are significant. **Eubanks (2018)** argues that digital financial systems can reinforce social inequalities through biased algorithms and exclusionary practices. Algorithmic bias, lack of transparency, and limited redress mechanisms can result in systemic disadvantages for marginalized groups.

Srivastava and Bansal (2021) suggest a rights-based approach to data protection, where personal data is treated not merely as an economic asset but as a facet of individual dignity and autonomy. The balance between fostering innovation and ensuring privacy protection is a delicate one, requiring a holistic approach that includes ethical design, responsible governance, and participatory regulation.

3. RESEARCH METHODOLOGY

This study adopts a **qualitative, descriptive research design**. It relies on **secondary data** collected from academic journals, government reports, industry whitepapers, legal statutes (such as the GDPR and India's DPDP Act 2023), and case studies of Fintech companies. Thematic content analysis is employed to categorize the data into key issues: regulatory adequacy, user awareness, technological vulnerabilities, and corporate responsibility. Comparative analysis is also used to examine privacy frameworks across different jurisdictions.

4. ANALYSIS

The analysis reveals several key themes:

4.1 Role of Judiciary

The Indian judiciary has played a pivotal role in developing a privacy-centric legal framework for digital finance. By affirming the right to privacy, scrutinizing regulatory overreach, and acknowledging the importance of digital access, the courts have attempted to strike a balance between technological innovation and constitutional rights. Long before the digital era, in *People's Union for Civil Liberties (PUCL) v. Union of India (1997)*, the Supreme Court recognized that telephone tapping violated the right to privacy. The principles laid down here foreshadowed the need for procedural safeguards in any form of surveillance, including financial surveillance through digital means.

The watershed moment for right to privacy in India came with the Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*, where a nine-judge bench unanimously declared the right to privacy a fundamental right under Article 21 of the Constitution. The Court emphasized that privacy includes informational self-determination, which is directly applicable to digital financial transactions. This decision laid the constitutional foundation for subsequent debates on data protection in the fintech sector. It imposed an obligation on both the State and private entities, including fintech companies to handle personal data with due care, consent, and accountability.

In *Binoy Viswam v. Union of India (2017)*, the petitioner challenged the government's directive to link Aadhaar with PAN cards for income tax filings. While the Court upheld the provision, it acknowledged

significant privacy concerns and insisted on procedural safeguards. This decision was pivotal in determining the legitimacy of Aadhaar-based e-KYC, which is widely used in fintech onboarding and identity verification. Further in *Internet and Mobile Association of India (IAMAI) v. Reserve Bank of India (2020),* the Supreme Court set aside the RBI's 2018 circular that prohibited banks from dealing with cryptocurrency exchanges. The Court ruled that the ban was disproportionate and infringed on the right to trade under Article 19(1) (g). This was a significant judgment for the crypto-fintech ecosystem, reinforcing judicial scrutiny over regulatory actions that could stifle innovation. The judgment established that financial innovation must be met with reasonable, not excessive, regulation, particularly when such innovation intersects with constitutionally protected freedoms.

As fintech continues to grow and integrate with other digital ecosystems—such as Aadhaar, UPI, and digital banking—it is imperative that judicial vigilance remains strong, particularly in ensuring that data protection principles are not sacrificed at the altar of convenience or growth.

4.2 Regulatory Gaps

India long lacked a comprehensive data protection framework, relying instead on fragmented provisions under the Information Technology Act, 2000 and rules thereunder. Though the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* (2017) recognized the right to privacy as a fundamental right, legislative responses have lagged behind. The recent enactment of the Digital Personal Data Protection (DPDP) Act, 2023 is a step forward, but sector-specific clarity for fintech remains absent. Fintech platforms often operate in regulatory grey areas, collecting sensitive data without adequate transparency, purpose limitation, or consent frameworks. A major challenge in the fintech ecosystem is the blurred line between regulated financial institutions (like banks and NBFCs) and unregulated fintech entities, such as app-based lenders, aggregators, or payment intermediaries. While banks are supervised by the Reserve Bank of India (RBI) and subject to stricter data handling norms, many fintech startups operate without robust oversight. This inconsistency results in uneven application of privacy safeguards**,** leading to potential misuse or unauthorized sharing of financial data.

Even where regulations exist, enforcement mechanisms are weak. For instance, the RBI's 2021 guidelines on digital lending were intended to curb predatory practices and protect consumer data. However, many app-based lenders continue to flout these norms, often bypassing regulations by partnering with shadow NBFCs or using complex ownership structures. Consumers have limited awareness or recourse, especially in the event of a data breach or unauthorized profiling.

Despite the introduction of India's Digital Personal Data Protection Act (DPDP), enforcement mechanisms remain weak, and ambiguities persist regarding data localization and consent management. Smaller Fintech startups often lack the capacity to implement advanced privacy protocols, unlike large institutions governed by GDPR or similar regulations.

4.2 Informed Consent and User Awareness

In theory, consent empowers users to make informed choices about how their personal and financial data is collected, used, and shared. Most fintech apps and platforms require users to accept terms and conditions and privacy policies before accessing services. However, this process is often opaque and perfunctory. Lengthy documents, usually written in legal or technical language, discourage users from engaging meaningfully with the content. As a result, users tend to accept all conditions without understanding the extent or consequences of data sharing, a phenomenon known as *"consent fatigue"*. Moreover, consent in many fintech platforms is often bundled, users cannot opt out of specific data practices without forfeiting the service entirely. This undermines the principle of granular, informed, and

voluntary consent, which is central to data protection frameworks such as the EU's GDPR or India's Digital Personal Data Protection (DPDP) Act, 2023. Most users are unaware of the extent to which their data is harvested, sold, or profiled. Consent is often bundled in unreadable terms of service. This violates the principle of "freely given, informed, and specific" consent mandated by international privacy norms.

Another critical issue is the low level of digital and financial literacy among a large section of fintech users. Many users are unaware of what data is being collected, how it is processed, and who it is shared with. This lack of awareness makes individuals vulnerable to exploitative practices, such as excessive profiling, behavioral targeting, or unauthorized data sharing with third parties. Fintech companies also make use of dark patterns, interface designs that subtly manipulate users into giving consent. For example, apps may highlight the *"Accept All"* option while hiding more privacy-conscious alternatives, or they may use confusing toggles to deter users from modifying data-sharing preferences.

Informed consent and user awareness are not just legal requirements, they are essential for building trust in digital finance. As fintech continues to expand, protecting user autonomy and promoting transparency must become central pillars of the data governance ecosystem.

4.3 Technological Risks

Fintech platforms, particularly those using AI, blockchain, or cloud computing, are susceptible to hacking, data breaches, and algorithmic bias. Data minimization and privacy-by-design principles are seldom prioritized in early-stage Fintech ventures. Fintech platforms store and process enormous volumes of sensitive personal and financial data, making them prime targets for cyberattacks. A single breach can expose not only users' financial credentials but also biometric identifiers, credit histories, and behavioral patterns. Despite this, many startups in the fintech sector lack the infrastructure or investment to implement robust cybersecurity measures, exposing users to risks of identity theft, fraud, and financial loss**.**

Technological innovation in fintech comes with inherent privacy and security risks that demand urgent attention. Without robust technical safeguards, ethical AI practices, regulatory oversight, and user education, the same technologies that democratize finance could also compromise personal liberty. A future-ready fintech ecosystem must be built not only on innovation but also on trust, transparency, and digital resilience.

4.4 Corporate Responsibility

A key aspect of corporate responsibility is ensuring that users are truly informed about how their data is collected, processed, and shared. Companies must avoid lengthy privacy policies or using dark patterns that nudge users into giving up personal information. Instead, fintech companies should offer clear, concise, and multilingual privacy notices, provide granular controls for data sharing preferences, and design user-friendly interfaces that empower informed decision-making. Corporate responsibility includes investing in robust cybersecurity infrastructure to protect user data from breaches, theft, and misuse. It includes educating users about digital finance, privacy risks, and data rights. Fintech firms should run awareness campaigns, build literacy tools into their apps**,** and partner with civil society to empower users with the knowledge to make informed financial decisions. As stewards of sensitive user data and drivers of financial inclusion, fintech companies bear a significant corporate responsibility to uphold privacy and protect user rights. By fostering a culture of transparency, accountability, and ethical innovation, they can not only mitigate risks but also contribute to a more trustworthy, inclusive, and sustainable digital finance ecosystem.

While some large Fintech firms follow international standards (e.g., ISO/IEC 27001), there is a general lack of uniform accountability mechanisms. Data protection officers and internal audits are not universally implemented, especially among emerging startups.

5. FINDINGS

1. Regulatory frameworks are evolving but are often reactionary and fragmented across jurisdictions.
2. User privacy is compromised due to insufficient consent models and lack of awareness.
3. Corporate compliance is uneven, with large firms leading the way and smaller players lagging.
4. Technological innovations, while beneficial, pose significant threats to privacy when not governed properly.
5. Public trust in Fintech depends on transparent data practices and strong legal enforcement.

6. CONCLUSION

As Fintech reshapes global finance, ensuring the right to privacy must be a policy priority. The current landscape is characterized by rapid innovation outpacing regulation, putting users at risk of data exploitation. Strengthening legal frameworks, enforcing compliance, encouraging ethical design, and enhancing digital literacy are critical steps forward. A privacy-first Fintech ecosystem not only protects individual rights but also builds trust and sustainability in digital finance.

7. 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. Bazarbash, M. (2019). **Fintech in Financial Inclusion: Machine Learning Applications in Assessing Credit Risk.** *IMF Working Paper No. 19/109*. International Monetary Fund.
3. Eubanks, V. (2018). **Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.** New York: St. Martin's Press.
4. Gai, K., Qiu, M., & Sun, X. (2018). **A Survey on Fintech.** *Journal of Network and Computer Applications*, 103, 262–273.
5. Liébana-Cabanillas, F., Marinkovic, V., & Kalinic, Z. (2017). **A SEM-neural network approach for predicting antecedents of m-commerce acceptance.** *International Journal of Information Management*, 37(2), 14–24.
6. Lee, I., & Shin, Y. J. (2018). **Fintech: Ecosystem, Business Models, Investment Decisions, and Challenges.** *Business Horizons*, 61(1), 35–46.
7. Radanliev, P., De Roure, D., Burnap, P., et al. (2020). **Artificial Intelligence and Cyber Risk to Financial Services.** *Technological Forecasting and Social Change*, 161, 120284.
8. Sharma, R. (2023). **India's Digital Personal Data Protection Act: A Critical Appraisal.** *Journal of Law and Technology*, 39(1), 51–68.
9. Solove, D. J. (2006). **A Taxonomy of Privacy.** *University of Pennsylvania Law Review*, 154(3), 477–564.
10. Srivastava, A., & Bansal, S. (2021). **Data Protection and the Ethics of Fintech: A Rights-Based Approach.** *Indian Journal of Law and Technology*, 17(1), 89–112.

11. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). **EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies.** *Computer Law & Security Review*, 34(1), 134–153.
12. Voigt, P., & von dem Bussche, A. (2017). **The EU General Data Protection Regulation (GDPR): A Practical Guide.** Springer International Publishing.
13. Xu, X., Chen, X., & Kou, G. (2019). **A Systematic Review of Blockchain.** *Financial Innovation*, 5(1), 1–14.
14. Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2020). **The Future of Data-Driven Finance and RegTech: Lessons from EU GDPR and Beyond.** *Journal of Financial Regulation*, 6(2), 174–203.
15. Narayanan, A., & Vallor, S. (2019). **Technology Ethics in Fintech: Analyzing Surveillance Capitalism.** *Ethics and Information Technology*, 21(4), 305–316.
16. Ramanathan, R. (2021). **India's Data Protection Law: An Analysis of the Draft Legislation.** *Economic and Political Weekly*, 56(12), 44–50.
17. OECD. (2022). **Digital Finance and Consumer Protection in the Age of Data.** *OECD Publishing.*
18. European Union (2018). **General Data Protection Regulation (GDPR).** *Official Journal of the European Union.*
19. Government of India (2023). **Digital Personal Data Protection Act.** *Ministry of Electronics and Information Technology.*
20. World Bank (2021). **Harnessing Fintech for Financial Inclusion and Human Rights.** *World Bank Publications.*
21. People's Union for Civil Liberties (PUCL) v. Union of India , AIR1997SC568
22. Justice K.S. Puttaswamy (Retd.) v. Union of India, 2019 (1) SCC 1
23. Binoy Viswam v. Union of India, WP(Civil) No. 277/2017
24. Internet and Mobile Association of India (IAMAI) v. Reserve Bank of India, AIRONLINE 2020 SC 298