Rethinking FinTech Regulation Under the Indian Data Protection Framework

Assistant professor **Amit Kumar KASHYAP**[1]

Abstract

This article examines the substantial implications of the Digital Personal Data Protection Act, 2023 (DPDPA) on the developing FinTech industry in India. With a principle-based approach, the DPDPA emphasises user control, accountability, and transparency in addressing critical issues in the data-driven FinTech sector. Combining doctrinal analysis and an exploratory methodology, this study meticulously investigates the Act's insight into obligations, focusing on the intricate distinctions between data processors and data fiduciaries. The objective of this doctrinal and exploratory analysis is to thoroughly comprehend the legal structure established by the Act, thereby clarifying the consequences for participants in the FinTech ecosystem. This study explores the DPDPA's impact on managing and safeguarding financial data within the dynamic FinTech sector. It accomplishes this through an evaluation of legal instruments and literature reviews. The paper concludes by suggesting changes to be taken by the financial regulator as a way to address concerns related to data security. Additionally, it initiates a discourse on the regulation of FinTech in India. It emphasises the significance of the collaboration between the Reserve Bank of India and the Ministry of Information Technology on data protection.

Keywords: *FinTech; data protection; privacy; personal sensitive data; information technology.*

JEL Classification: K22, K23

DOI: 10.62768/TBJ/2024/14/3/02

Please cite this article as:	**Article History**
Kashyap, Amit Kumar, 'Rethinking FinTech Regulation Under the Indian Data Protection Framework', *Juridical Tribune – Review of Comparative and International Law* 14, no. 3 (October 2024): 363-383.	Received: 10 March 2024 Revised: 7 May 2024 Accepted: 15 June 2024

1. Introduction

Technology has been involved with financial services since the 1850s. Still, "FinTech" has just been popularised in the last 20 years to characterise innovations that might change how financial services are provided.[2] New consumer goods, services, and business models may emerge due to these innovations.[3] FinTech refers to

[1] Amit Kumar Kashyap - Centre for Corporate Law Studies, Institute of Law, Nirma University, Ahmedabad, India, amit1law@gmail.com, https://orcid.org/0000-0002-2716-8482.

[2] Murinde, Victor, Efthymios Rizopoulos, and Markos Zachariadis. "The impact of the FinTech revolution on the future of banking: Opportunities and risks." *International review of financial analysis* 81 (2022), p. 102-103.

[3] Ibid

using technology to digitise and automate banking and financial services, including bank accounts and ledgers, using innovative and unconventional methods.[4] FinTech can be defined as a market function, institutions, technology, structure, impact, and disruption.[5] Many markets and authorities, particularly in the United States and the United Kingdom, had a laissez-faire approach towards financial innovation before the 2008 financial crisis.[6] However, a change towards strict regulatory measures, precipitated by the crisis, reversed this tolerant stance. So, there was a boom in FinTech, which includes new and old financial institutions and digital companies.[7]

As a result of policies brought into effect following the financial crisis, a new industry called FinTech has evolved, mirroring the long-standing relationship between technology and money. Changes occur quickly, and new players from all walks of life are entering the financial sector in this new FinTech age. Opportunities for innovation are created when conventional institutions, tech giants and startups compete in global marketplaces. The growing number of FinTech firms and the increasing adoption by customers in recent years have highlighted the need for robust data security solutions to protect sensitive information.[8] Such precautions are critical in the modern digital era for preserving consumer confidence and reducing the likelihood of data breaches.

After the 2008 crisis, lending ethics must be improved by swift, accurate loan reviews, which Fintech makes easier. Progress typically requires collecting a lot of data.[9] Fintech is making progress thanks to big data, which uses computer information to predict how people will act. Personalized banking ideas, credit checks, scam detection, and focused marketing show Fintech's data-driven method. Still, worries about data security breaches, the responsibility of automatic decision-making, and the protection of consumer rights in this changing environment loom large.

Therefore, fintech companies must prioritize data security to protect their customers and customers' information against unauthorized access. This requirement is particularly critical since FinTechs have become major global financial services industry participants over the last decade. Numerous data-related challenges confront fintech firms, including assuring data discoverability, managing encryption complexities, and adhering to regulatory compliance standards.[10] Securing data within

---

[4] Bilotta, Nicola, and Simone Romano. Tech Giants in Banking: The Implications of a New Market Power. Istituto Affari Internazionali (IAI), 2019. JSTOR, http://www.jstor.org/stable/resrep19672. Accessed 21 Mar. 2024.

[5] Walker, George. "International Law: Financial Technology Law: A New Beginning and A New Future." *GP Solo* 34, no. 3, 2017, p. 76-77.

[6] Tonveronachi, Mario. "Ending laissez-faire finance." Corsi M., Kregel J. e D'Ippoliti C.(a cura di), *Classical Economics Today. Essays in Honor of Alessandro Roncaglia* (2018): 19-32.

[7] Arner, Douglas W., et al. "FinTech and RegTech: Enabling Innovation While Preserving Financial Stability." *Georgetown Journal of International Affairs*, vol. 18, no. 3, 2017, pp. 47–58. JSTOR, http://www.jstor.org/stable/26395923. Accessed 21 Mar. 2024.

[8] Stewart, Harrison, and Jan Jürjens. "Data security and consumer trust in FinTech innovation in Germany." *Information & Computer Security* 26.1, 2018, p. 109-128.

[9] Gomber, Peter, et al. "On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services." *Journal of management information systems* 35.1, 2008, p. 220-265.

[10] Akanfe, Oluwafemi Adeola. *Advancing Digital Financial Inclusion: Data Privacy, Regulatory Compliance, and Cross-Country Cultural Values in Digital Payment Systems Use*. Diss. The University

lending FinTechs is contingent upon consistently implementing preventive measures to prevent potential misuse. It is critical for fintech companies to thoroughly assess cybersecurity risks linked to software-as-a-service (SaaS) applications and maintain a vigilant awareness of the ever-changing data regulations and compliance requirements.[11]

Fintech firms manage sensitive customer data and financial transactions, necessitating robust security measures. Fundamental principles in this arena include prioritizing trust, ethics, and culture. Compliance with ESG standards underscores a commitment to responsible governance. Security must be integrated into fintech solutions from inception, with regular testing to ensure resilience. Adherence to global regulations like GDPR and CCPA grants consumers control over their data.[12] Balancing innovation with security, especially with technologies like blockchain and AI, is paramount. Ultimately, prioritizing data protection and fostering trust is vital for long-term success in the fintech sector.

Fintech is widely regarded as a driving force behind the expansion of financial inclusion in India, offering novel solutions and alternative approaches to conventional banking practices.[13] With notable developments in digital payments and cutting-edge technology like blockchain, machine learning, and cloud computing, India is the world leader in adopting Fintech.[14] The Covid-19 epidemic in India has significantly increased digital transactions, primarily because of the FinTech industry.[15] This sector has provided online payment channels to facilitate seamless transactions. The current exceptional circumstances have prompted the growth of digital payment markets. The nation is now experiencing a significant fintech boom, and it is home to the second-largest fintech centre in the world—only exceeded by the US.[16] India is a world leader in Fintech acceptance, with an astounding rate of 87%, because of its abundant smartphone usage and internet accessibility.[17] Currently, 21 of the 187 unicorns in the financial industry are from India.[18] Paytm, PhonePe, and Google Pay have all

of Texas at San Antonio, 2022.

[11] Morosanu, Georgiana-Alexandra, Laura Andreea Rata, and Marius Geru. "Aspects Regarding CyberSecurity Developments on SaaS Software Platforms." *EIRP Proceedings* 18.1, 2023, p. 128-146.

[12] Bakare, Seun Solomon, et al. "Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations." *Computer Science & IT Research Journal* 5.3, 2024, p. 528-543.

[13] Salampasis, Dimitrios, and Anne-Laure Mention. "FinTech: Harnessing innovation for financial inclusion." *Handbook of blockchain, digital finance, and inclusion*, volume 2. Academic Press, 2018. 451-461.

[14] Kukreja, Gagan, Divij Bahl, and Ruchika Gupta. "The impact of Fintech on financial services in India: Past, present, and future trends." *Innovative strategies for implementing Fintech in banking*. IGI Global, 2021. 191-200.

[15] Savitha, Basri, Iqbal Thonse Hawaldar, and Naveen Kumar. "Continuance intentions to use FinTech peer-to-peer payments apps in India.", 2022, *Heliyon* 8.11.

[16] G. Singh, R. Gupta and V. Vatsa, "A Framework for Enhancing Cyber Security in Fintech Applications in India," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 274-279, doi: 10.1109/ICTAI53825.2021.9673277

[17] Andrae, Silvio. "The role of BigTech in emerging markets." In *Handbook of Banking and Finance in Emerging Markets*, Edward Elgar Publishing, 2022. pp. 433-463.

[18] Bhura, Pawan, and Sanjeev Bansal. "Current Status, Trends & Prospects of FinTech in India." *International Journal of Management, Public Policy and Research* 2.4 (2023): 131-138.

contributed significantly to the nation's popularity of digital payments.[19] Although Fintech is expanding rapidly in India, it encounters challenges such as the digital divide, cybersecurity risks, regulatory uncertainty, and data privacy concerns. Since competition is intensifying, this development also creates prospects for cooperation and innovation. Fintech firms can establish sustainable business models by collaborating with conventional financial institutions and catering to various customer requirements. The financial technology sector is undergoing fast development, emphasising the need for cybersecurity measures to preserve trust and sustainability. Fintech companies, which manage intricate financial systems and process substantial amounts of consumer data, are susceptible to cyber-attacks. In 2023, cybercrimes, compliance with regulations, cooperation, and innovative technologies like blockchain, artificial intelligence, and machine learning will all play significant roles in creating a secure environment in the financial technology industry. These technologies make data interpretation, discovering anomalies, and accurate threat intelligence easier. Fintech firms face challenges for privacy and data security, regulatory compliance, third-party supplier risk mitigation, and human-related issue resolution. International companies experience pretty much a challenge in complying with data security laws like GDPR and local statutes. Protecting customer information and the financial system's stability depends on effective risk management in cybersecurity. The sensitive nature of the data collected by fintech businesses necessitates extra precautions. The words "privacy" and "security" are not synonymous. The former speaks of consumers' ability to manage how their data is used, and the latter is data security against outside dangers.

The Digital Personal Data Protection Act of 2023 (DPDPA) creates a legislative framework regulating digital personal data gathering and use in India.[20] Adopting this has significant consequences in other areas, including Fintech, which previously lacked regulation. The Act seeks to balance the promotion of fintech innovation with the need to protect data privacy. Despite its well-meaning goals, the DPDPA's directions conflict with the current fintech rules, such as the Reserve Bank of India's 2022 Guidelines on Digital Lending.[21] The article examines the impact of the DPDPA on the privacy practices of FinTech firms.

This study aims to comprehensively analyse the data protection compliance of fintech companies in India. Nevertheless, the precise objective of this research is to address a knowledge gap by examining the policy and legal concerns surrounding compliance with data protection regulations in the fintech sector. Additionally, it seeks to trace the historical progression of data protection legislation in India and other developing nations that influence the fintech industry. At the same time, the DPDPA is

[19] Macierzyński, Wiesław Łukasz, and Michał Macierzyński. "Development of new payment services and the role of the fintech sector during the COVID-19 pandemic." *Central European Review of Economics & Finance* 44.3 (2023): 61-78.

[20] Sundara, Karishma, and Nikhil Narendran. "The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection." *Computer Law Review International* 24.5, 2023, p. 129-141.

[21] Ibid.

not yet in force in India.

2. Literature review

Fintech has been seen as the close cooperation between financial services and information technology in the last decade.[22] The US Global Financial Crisis has been one of the precursors of digitalisation and decentralisation of financial services, making Fintech a new norm.[23] Because there isn't yet a specialised regulatory structure that takes into account the unique complexities of the financial technology industry, companies in this field are understandably anxious about government oversight.[24] The fast development of Fintech, including innovations like digital assets and cryptocurrencies, has led many to believe that traditional regulatory measures are reactive and insufficient.[25]

The fintech companies confront multiple challenges in ensuring data security and complying with ethical standards.[26] The absence of universally accepted standards for protecting data creates obstacles to securing global confidentiality for customers.[27] Further, the transfer of personal data across borders gives rise to issues related to regulation, emphasising the importance of an international regulatory structure on data privacy. This is further illustrated by the impacts of the General Data Protection Regulation (GDPR) on privacy laws in the fintech industry.[28] The importance of protecting consumer data and adhering to data protection regulations is emphasized by ethical issues, which recommend straightforward measures such as adopting encryption techniques and ensuring transparent data usage.[29] Legal problems associated with using personal data in fintech services are data privacy and security, emerging tech, cybersecurity, and financial threats,which calls for the responsibility of fintech operators to safeguard the customer data and the possible legal repercussions for any data abuse.[30] Furthermore, adopting robust safety protocols such as the Secure

[22] Ashta, Arvind, and Guillaume Biot-Paquerot. "FinTech evolution: Strategic value management issues in a fast changing industry." *Strategic Change* 27.4 (2018): 301-311.
[23] Setiawan, Kukuh, and Nadia Maulisa. "The evolution of fintech: a regulatory approach perspective." 3rd International Conference on Law and Governance (ICLAVE 2019). Atlantis Press, 2020.
[24] Zheng, Yulu, and Xiaoli Wu. "Fostering fintech innovation: A tripartite evolutionary game analysis of regulatory sandbox experiments." *International Review of Economics & Finance* (2024).
[25] Stefanelli, Valeria, and Francesco Manta. "The rise of digital finance: empirical evidence on fintech firms, banks and customers." (2022): 1-121.
[26] Alekseenko, Aleksandr P. "Privacy, Data Protection, and Public Interest Considerations for Fintech." *Global Perspectives in FinTech: Law, Finance and Technology.* Cham: Springer International Publishing, 2022. 25-49.
[27] Hernández, Elena, et al. "Data protection on FinTech platforms." *Highlights of Practical Applications of Survivable Agents and Multi-Agent Systems*. The PAAMS Collection: International Workshops of PAAMS 2019, Ávila, Spain, June 26–28, 2019, Proceedings 17. Springer International Publishing, 2019.
[28] Dorfleitner, Gregor, Lars Hornuf, and Julia Kreppmeier. "Promise not fulfilled: FinTech, data privacy, and the GDPR." *Electronic Markets* 33.1 (2023): 33.
[29] Aldboush, Hassan HH, and Marah Ferdous. "Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust." *International Journal of Financial Studies* 11.3 (2023): 90.
[30] Devianti, Dwi Nugrahayu, Prija Djatmika, and Sukarmi Sukarmi. "The Risks of Personal Data Theft in

Hash Algorithm (SHA) and Advanced Encryption Standard (AES) could successfully deal with security and privacy concerns in the financial sector.[31]

Critical constraints to effective regulation include legal challenges, contributing to the regulatory issue of striking the right balance between fintech innovation, risk prevention, and financial stability.[32] Organisations that deal with user data must adhere to security standards, and unethical conduct stems from fraud, mistreatment, or unfair treatment of users. Data privacy, AI regulatory frameworks, and cybersecurity are all at risk from emerging technologies like AI. Corporations must comply with Know Your Customer rules to avoid penalties and litigation related to cybersecurity, which threatens financial operations and user data.

In recent years, India's diversified fintech ecosystem—which includes startups, tech businesses, banks, and non-banking financial organisations—has seen tremendous development.[33] Although there continue to be challenges to overcome, India's fintech ecosystem is going through an evolution that provides companies with a platform for economic growth.[34] Cybersecurity, data protection, and consumer protection are three areas where India's rapidly expanding fintech industry has created obstacles to regulation. [35] The Facebook data leak and suspected Aadhar data breach have brought attention to the immediate need for data security measures in India's fintech industry.[36] The introduction of the DPDPA in India was prompted by the need to address the many challenges and concerns faced by e-commerce companies and consumers. This Act draws inspiration from the EU's General Data Protection Regulation (GDPR) and attempts to provide a robust legal framework for data protection in India.[37]

The DPDPA is a substantial legislative measure in India that is designed to protect personal data, encompassing financial and physical information. The legislation was implemented in August 2023 as a response to the IT Act of 2000's inadequate emphasis on data privacy.[38] The regulation about handling digital personal

---

Fintech-Based Online Loan Applications Due to the Absence of Law in Indonesia." *Jurisdictie: Jurnal Hukum dan Syariah* 11.2 (2020): 163-181.

[31] Thakur, Nikita, and Vandana Sharma. "Enhancing Fintech Security-A Comparative Analysis of Advanced Security Algorithms." 2023 2nd International Conference on Edge Computing and Applications (ICECAA). IEEE, 2023.

[32] Minto, Andrea, Moritz Voelkerling, and Melanie Wulff. "Separating apples from oranges: Identifying threats to financial stability originating from FinTech." *Capital markets law journal* 12.4 (2017): 428-465.

[33] Ramkumar, Gowtham. "FinTech in India: A systematic literature review." *The sustainable Fintech revolution: Building a greener future for finance* (2023): 225-250.

[34] Baporikar, Neeta. "Fintech challenges and outlook in India." *Innovative strategies for implementing FinTech in banking*. IGI Global, 2021. 136-153.

[35] Singh, Gurinder, Ruchika Gupta, and Vidushi Vatsa. "A framework for enhancing cyber security in fintech applications in india." 2021 International Conference on Technological Advancements and Innovations (ICTAI). IEEE, 2021.

[36] Ibid.

[37] Prasad M, Deva, and Suchithra Menon C. "The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law." *International Journal of Law and Information Technology* 28.1 (2020): 1-19.

[38] Naithani, Paarth. "Regulating artificial intelligence under data protection law: Challenges and solutions

data within India applies to such data, even if it is processed outside of India and is connected with Indian products or services.[39] It mandates individuals to provide unambiguous consent and permits the revocation of consent. The DPDPA mandates data deletion, breach prevention measures, reporting to authorities, data accuracy, and outlining data rights, obligations, and transfer regulations.[40] It enables international data transfer that is subject to governmental restrictions.[41] Fintech firms must alter data handling to comply, potentially increasing operational complexity but necessitating innovative approaches like advanced data anonymization techniques to balance privacy and analysis requirements.[42]

3. Research methodology

This article uses a combination of doctrinal and exploratory research methods to examine the implementation of the Data Protection Bill and its impact on fintech enterprises in India. The doctrinal research component involves a thorough analysis of legal materials, such as the Data Protection Law, relevant legislative papers, case law, and regulatory directives. This article aims to elucidate the legal framework established by the legislation, scrutinise its sections, and appreciate its impact on fintech data protection processes.

To improve the study of doctrine, an exploratory technique will be used to get insight into the practical implications. The potential impacts of the Data Protection Bill on fintech operations, innovation, and service delivery will be assessed and scrutinised in industry papers, policy briefs, and academic literature.

The following Legal Instruments have been referred for analysis of data protection compliance for FinTechs in India:

- Information Technology Act 2000
- Digital Personal Data Protection Act, 2023
- Payment and Settlement Systems Act of 2007
- Companies Act, 2013
- Consumer Protection Act of 2019
- Prevention of Money Laundering Act, 2002
- Banking Regulation Act, 1949
- Insurance Regulatory and Development Authority of India Act, 1999
- Credit Information Companies (Regulation) Act, 2005

for India." *Indian JL & Just*. 14 (2023): 436.

[39] Oyewole, Adedoyin Tolulope, et al. "Data privacy laws and their impact on financial technology companies: a review." *Computer Science & IT Research Journal* 5.3 (2024): 628-650.

[40] Kashyap, Amit Kumar, and Mahima Chaudhary. "Cyber security laws and safety in e-commerce in India." *Law & Safety* (2023): 207.

[41] Shehu, Vlona Pollozhani, and Visar Shehu. "Human rights in the technology era–Protection of data rights." *European Journal of Economics, Law and Social Sciences* 7.2 (2023): 1-10.

[42] Pandey, Sharad Kumar, and Ravi Dubey. "Critical Analysis of Role of Data Protection In The Growth Of Fintech at Global Regime Including India." *Journal of Research Administration* 5.2 (2023): 9538-9553.

- Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983
- Income Tax Act, 1961
- EU General Data Protection Regulations 2016

To identify and address legal deficiencies, the research employed a doctrinal legal approach and comparative analysis to examine other jurisdictions' policies, laws, and experiences regarding data protection and its ramifications for Fintech through international legal instruments and methods. This paper assesses the effectiveness of international legal instruments and frameworks from the EU in analysing data protection law compliance issues within the fintech industry.

4. Results

4.1. Legal & security framework for FinTech in India

The fintech industry in India has grown significantly in the last several years due to changes in consumer behaviour, greater internet penetration, and technical improvements. The legal and security framework governing fintech activities becomes essential as the industry evolves continuously. The regulatory environment governing fintech activity in India is complex, with many laws governing data protection, consumer rights, and financial transactions.[43] The lack of uniform FinTech rules creates substantial issues for regulation and monitoring. The following sections outline significant legislation that affects FinTech activities in India.

Legal Instruments	Purpose
Payment and Settlement Systems Act of 2007 (PSS Act)	Payment systems are defined under the PSS Act as those that permit money transfer, credit card, debit card, or smart card activities. Unless a court or other legal body rules otherwise, providers must keep the documents and information they receive from system participants secret.
Companies Act, 2013	FinTech enterprises must adhere to the Companies Act of 2013, which requires registration and compliance with statutory duties.
Consumer Protection Act of 2019	The Consumer Protection Act classifies FinTech enterprises as service providers. Compliance is required to prevent unfair business practices, such as the unauthorized sharing of customer data.
Prevention of Money Laundering Act, 2002	The Prevention of Money Laundering Act and Rules and KYC guidelines create anti-

[43] Marda, Vidushi, and Amber Sinha. "FinTech Lending in India: Taking Stock of Implications for Privacy and Autonomy." *Indian Journal of Law and Technology*, vol. 18, no. 1, 2022, pp. 100-126. HeinOnline, https://heinonline-org.elibrary.nirmauni.ac.in/HOL/P?h=hein.journals/indiajoula18&i=106.

	money laundering requirements that apply to financial service providers.
The Information Technology Act of 2000	Compliance with data privacy requirements, under section 43A of the Information Technology Act of 2000, is critical for FinTech organizations that handle sensitive personal information.
Regulations of the Reserve Bank of India	The RBI controls various FinTechs directly or indirectly via NBFC licences, guaranteeing compliance with statutory standards.
Department for Promotion of Industry and Internal Trade ("DPIIT")	DPIIT has liberalized financial services FDI. 100% FDI in 'other financial services' is allowed automatically without government permission. This eases access to overseas investment without hassle.
The Insurance Act 1938	India's Insurance Regulatory Development Authority regulates insurance firms, notably those that provide online aggregator services.
The Foreign Exchange Management Act 1999	Cross-border transaction services in FinTech are governed by the Foreign Exchange Management Act, which includes requirements for prepaid payment instruments.
International Financial Services Centres ("IFSCs")	IFSCs are financial services-specific economic zones where registered businesses are legally recognized as foreign entities. They provide foreign currency financial services to residents and non-residents. Investors may smoothly invest in India under the IFSC framework without complying with Indian foreign currency regulations under the International Financial Services Centres Authority ("IFSCA").

Compliance with these standards is critical for FinTech businesses to function within the legal framework while ensuring consumer protection and financial integrity. Significant regulatory agencies that oversee various fintech operations, from payment systems and digital wallets to investment platforms and Insurtech solutions, include the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI), and Ministry of Electronics and Information Technology (MeitY). Non-Banking Financial Companies (NBFCs) regulations also affect fintech lenders, emphasizing the need to adhere to specific legal requirements.

4.2. Issues & challenges in FinTech regulation

Authorities must take action to protect the stability of these institutions and preserve market integrity due to the many challenges that arise from the regulatory and supervisory components of FinTech activities. The ever-changing FinTech sector needs immediate legislative changes to regulate financial institutions better. Effective conduct control and prudential regulation are crucial to maintaining market integrity. All of these initiatives are a component of the new micro-tech regulatory structure.

In India, complex FinTech regulation refers to the coexistence of services and laws from many jurisdictions. This complexity calls for yearly legislative changes and new legislation to manage evolving concerns. There is an uncertain regulatory environment since regulatory bodies always look for gaps and repercussions in the service offered. FinTech companies struggle to comply with the quick changes in regulations.

Regulatory Challenges: FinTech companies in India have difficulties in complying with regulations owing to the absence of a comprehensive regulatory framework, dynamic legislative changes, and the need for regular approvals. FinTech companies face significant compliance obstacles due to the decentralised regulatory structure.

Data Protection & Privacy: Data Protection & Privacy pose significant challenges in FinTech. Data privacy breaches pose a substantial risk to the regulatory compliance, financial stability, and reputation of FinTech organisations. Digital business methods make vulnerable consumer data accessible. Hence, it is essential to implement stringent measures to prevent data breaches and fraudulent activities.

KYC Compliance Challenges: Verifying KYC (Know Your Customer) requirements mandated by the RBI (Reserve Bank of India) involves extensive data gathering, storage, and monitoring, necessitating a substantial financial commitment. FinTech companies have challenges allocating resources to meet regulatory compliance standards due to stringent regulations.

Cybersecurity Threats: FinTech organisations have increased susceptibility to malware, phishing, ransomware, and DDoS attacks due to the digitization of the financial industry. FinTech platforms must safeguard client data and maintain trust by implementing robust cybersecurity measures.

Insider Threat: The security of data is at risk due to unauthorised access or malevolent behaviour carried out by employees, contractors, or partners. Implementing access restrictions, implementing monitoring systems, and providing staff training may help mitigate insider threats, such as data theft, fraud, and sabotage.

Risks from External Parties: FinTech firms rely on third-party providers for cloud hosting, payment processing, and customer support, which introduces security concerns. Efficient risk management requires thorough investigation, contractual safeguards, and monitoring of third-party vendor compliance.

Global Compliance: FinTech firms in India must adhere to the General Data Protection Regulation (GDPR) and the Personal Data Protection Bill (PDPB) to ensure data privacy and comply with regulatory standards. Minimise the risk of legal

complications by adhering to strict regulations on data collection, processing, storage, and sharing.

Financial Data Localization: In some nations, financial data must be stored and processed inside their borders, restricting the transmission of sensitive information. Due to data localisation regulations, FinTech's in different countries must establish local data storage and infrastructure.

Regulatory Challenges: FinTech companies operating in India must confront and resolve the challenges posed by regulations to adhere to data protection and Know Your Customer (KYC) regulations. Proactive adherence to rules and ensuring data security are essential for the sustainable growth of FinTech.

These challenges show that FinTech is the convergence of technology and finance, leading to new ideas and opportunities. Digital technology must be employed for various financial purposes to guarantee safe transactions and accurate record-keeping. The introduction of innovative digital entitlements has made the transition from conventional to digital rights inescapable. Data breaches, phishing, and ransomware are examples of ever-changing cyber dangers in the Fintech industry, necessitating more excellent security standards. Fintech organisations must strengthen their defensive measures against cyberattacks by adding encryption, multi-factor authentication, and frequent audits. The Facebook data leak and the reported Aadhar data breach underscore the importance of data security in India's FinTech sector.[44] Therefore, it is crucial to safeguard online operations by implementing strategies at the individual user level and inside financial systems to minimise the impact of cyber-attacks.[45]

4.3. Data protection & FinTech

Data privacy and protection are gaining importance in the digital age as organizations must safeguard individuals' sensitive information from unauthorized access and misuse to build trust and security online.

India's IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011(SPDI Rules) regulate data privacy. Passwords, financial information, physical, physiological, mental health conditions, sexual orientation, medical records, and biometric information are just a few of the personal or sensitive data collectors required by the SPDI Rules to collect and process.

Data collectors are held responsible under Section 43-A of the IT Act for carelessness in putting in place and maintaining sufficient security measures and protocols for private information. If the data collector's carelessness causes unjustified loss or gain, the impacted party, especially the pertinent data subject, may be entitled

[44] Zhang, Xichen, et al. "Data breach: analysis, countermeasures and challenges." *International Journal of Information and Computer Security* 19.3-4, 2022, p. 402-442.

[45] Mohan, N., G. Rajasekar, and Ratno Agriyanto. "Anti-Fraud AI for Banking and FinTech Used in a Proactive Banking Strategy to Thwart SIM Phishing." *The Impact of AI Innovation on Financial Sectors in the Era of Industry 5.0.* IGI Global, 2023. 171-183.

to damages. The IT Act's Section 72-A addresses personal data and penalties for information disclosed against a legal contract or without the data subject's permission. India's Ministry of Electronics and Information Technology introduced the Digital Personal Data Protection Bill, 2022 (DPDP Bill) to simplify personal data management after repealing the PDP Bill.[46] The administration claims the law protects personal data, but a deeper look shows other ramifications. After becoming legislation, DPDPA covers legal data handling, data collecting limits, data reduction, storage, and data processor accountability.[47] Besides creating trust between persons and companies managing their data, the Act takes numerous more steps.

Indian fintech companies increasingly recognise the significance of adhering to global regulations such as GDPR and AML requirements. The GDPR and AML directives pose challenges for complying with domestic laws, particularly for firms handling data from the EU.[48] Compliance with GDPR is crucial for organizations managing the data of EU customers and users due to its stringent data protection measures, thereby adding to regulatory intricacies.[49] The DPDPA in India amalgamates local regulations with international data protection norms, mandating fintech enterprises to ensure compliance in regional and global markets.

About the right to correct, delete, and withdraw consent, there is an unambiguous expression in the DPDPA. These are among the three main instances in which consumers need to be able to ask questions about their personal information and express their desire to have part of it changed or removed. That is uncommon nowadays, as consumers are not given the option.

The Act identifies two distinct roles for managing data by Fintech Companies:

- *Data fiduciaries* are individuals or organizations entrusted with full responsibility and liability for data principals' data as defined in the Act.
- *Data processors* are responsible for handling the data on behalf of data fiduciaries, with obligations outlined in their contractual agreements.

Before taking any further steps, participants within the FinTech sector must determine whether they fall under the category of processors or fiduciaries. Many FinTech companies are involved in nonbanking activities and provide services to traditional banks and non-banking entities. The distinction between these roles depends on the activities involved and hinges on whether the entity is collecting or processing the data. Therefore, it is crucial to establish the entity's nature before developing and implementing procedures to comply with the Act.

For example, if a service provider is processing data on behalf of a bank's customers, it operates as a processor; however, if the same provider collects data from

---

[46] Sundara, Karishma, and Nikhil Narendran. "Protecting Digital Personal Data in India in 2023: Is the lite approach, the right approach?." *Computer Law Review International* 24.1, 2023, p. 9-16.

[47] Bareh, Chanlang Ki. "Reviewing the Privacy Implications of India's Digital Personal Data Protection Act (2023) from Library Contexts." *DESIDOC Journal of Library & Information Technology* 44.1, 2024.

[48] Bugeja, Diane. "AML/CFT and data privacy regulation: Achieving a peaceful co-existence." *Journal of Financial Compliance 2.2*, 2018, p. 132-141.

[49] Yadav, Yesha. "Fintech and International Financial Regulation." *Vanderbilt Journal of Transnational Law*, vol. 53, no. 3, May 2020, pp. 1109-1146. HeinOnline, https://heinonline-org.elibrary.nirmauni.ac.in/HOL/P?h=hein.journals/vantl53&i=1135.

its employees, whether for training AI models or other authorized purposes, it serves as a fiduciary.

Companies that handle digital data are legally obligated to guarantee the secure collection, processing, and sharing of personal data acquired from their customers, as the DPDPA mandates. Platforms are required by law to incorporate "reasonable security safeguards" to mitigate the risk of data breaches. Noncompliance may give rise to fines of no more than Rs 250 crore, and recurrent infractions may cause service disruptions. Companies entrusted with user data are responsible for safeguarding individuals' information, and any personal data violations must be reported immediately to the Data Protection Board (DPB).

4.4. Other regulations for data security

In India, many laws, such as the IT Act, banking secrecy laws, and regulatory regulations, establish the need to maintain data confidentiality and secrecy.[50] According to these provisions, data may be sent to other countries as long as the target country is not on the blocklist of the Indian Central Government. Nevertheless, if sector-specific legislation enforces more stringent criteria for transferring personal data outside of India, such restrictions will be given priority.[51]

The Reserve Bank of India (RBI) requires banks and payment system providers to ensure that payment transaction data is stored inside India and restrict its storage outside the country.[52] The Public Financial Institutions Act of 1983 forbids public financial firms from revealing customer information.[53] The Banking Regulation Act of 1949 regulates the gathering, storage, and protection of client data[54], while the Credit Information Act of 2005 dictates how credit information businesses handle data, including access, confidentiality, accuracy, and disclosure requirements.[55]

The Bankers' Book Evidence Act of 1891 restricts bank executives from disclosing bank records unless done in a court of law and for particular purposes. According to the Insurance Regulatory and Development Authority of India Act of 1999, insurance companies must protect policyholders' information.[56] They may only provide it to authorised government bodies when necessary. The Prevention of Money

[50] Jamil, Danish, and Muhammad Numan Ali Khan. "Data protection act in India with compared to the European Union countries." *International Journal of Electrical & Computer Sciences* 11.06 (2011).
[51] Duraiswami, Dhiraj R. "Privacy and Data Protection in India." *Journal of Law & Cyber Warfare* 6.1 (2017): 166-186.
[52] Garg, Hemant. "Financial Regulators and the Need for Data Privacy and Protection-Issues, Opportunities and Challenges." *International Journal of Legal Developments and Allied Issues* 8.1 (2022): 290-301.
[53] Mathew Martin, P. J., and Manukonda Rabindranath. "Digital Inclusion for access to information: A study on banking and financial institutions in India." SAGE Open 7.3 (2017): 2158244017720479.
[54] Dutta, Biswadeep. "Bank Licensing in India Defined under Banking Regulation Act 1949: Banking Sectors Journey throughout the Past and the Way Ahead in Future." *Indian JL & Legal Rsch*. 2 (2021): 1.
[55] Bali, Vinita. "Data privacy, data piracy: Can India provide adequate protection for electronically transferred data." *Temp. Int'l & Comp. LJ* 21 (2007): 103.
[56] Sastry, V. S. "Indian Insurance Data Issues." Seminar on “Data Base Issues in Financial Sector”. 2010.

Laundering Act of 2002 allows regulatory authorities to seek the disclosure of data[57] under the terms of the IT Act and SPDI Rules including the personal sensitive data compliance reporting.[58] Finally, the Income Tax Act 1961 establishes guidelines for safeguarding transaction-related information.[59]

4.5. Data protection laws in the EU

In May 2018, the European Union (EU) implemented the General Data Protection Regulation (GDPR) to strengthen individual rights and give companies handling personal data more accountability.[60] The primary goals of the GDPR are to increase personal information control for people, improve data protection procedures, and harmonise data protection legislation within the EU.

As considerable volumes of personal data are gathered and processed by the FinTech sector, which primarily depends on data-driven operations and analytics, including transactional details, personal identifying data, and financial information about customers, data protection compliance becomes foreseeable. Essential parts of the GDPR law that affect the FinTech industry in the EU include supplier management, pseudonymisation, customer permission, biometrics as financial transaction identifiers, the right to be forgotten, and disclosure of security breaches:

- Companies must get customer consent before disclosing personal data, including distinctive components of an individual's identity, and clarify why the data is being collected.

- Financial services are increasingly identifying their clients via biometrics; hence, regulations must be in place to keep them safe. A signaturist's electronic signature is offered as the ideal way to get clear and/or explicit permission, turning implicit consent into unambiguous, affirmative actions with complete legal assurances.

- The GDPR also gives every EU citizen the "Right to be forgotten," which allows them to ask financial institutions to erase their personal data. Financial institutions are permitted to retain any data to fulfil other legal requirements; however, in all situations where there is no good reason to maintain the data, the right to be forgotten shall take precedence.

- Companies have 72 hours to notify the supervisory authority of any data breach, together with information on the kind of incident, the categories and estimated number of impacted individuals, and the contact details of the Data Protection Officer. Organisations that provide services to EU residents or collaborate with EU banks must also ensure vigilance when exchanging data across borders.

---

[57] Hooda, Sneha. "Prevention of Money Laundering Act 2002: An Analysis from Lens of Principles of Law of Evidence." Issue 5 *Int'l JL Mgmt. & Human.* 3 (2020): 997.

[58] Pandey, Anoop Kumar. "Introduction to healthcare information privacy and security concerns." *Security and privacy of electronic healthcare records: Concepts, paradigms and solutions* (2019): 17-42.

[59] Krishna, Raj. "Data Management in India: A Case Study of Aadhaar Project." *Application of Big Data and Business Analytics*. Emerald Publishing Limited, 2020. 127-138.

[60] Goddard, Michelle. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact." *International Journal of Market Research* 59.6 (2017): 703-705.

- Another GDPR area where businesses must safeguard extra data that may be associated with a person but cannot directly identify them is pseudonymization. Companies are encouraged under the GDPR to pseudonymize data by removing identities, lowering processing risks while preserving data usefulness.

GDPR non-compliance has even harsher penalties than did the previous law. Companies will face penalties of €20 million, or 4% of their revenue; fines for less severe violations will be 2% of the total turnover. Apart from possible harm to reputation and loss of future business, these economic punishments.

5. Discussion

In its pursuit of expansion, the Fintech sector in India faces several challenges, including the need to engage with the unbanked population, navigate complex regulatory frameworks, integrate cutting-edge technologies, and improve the user experience. Addressing challenges such as restricted access to banking infrastructure, insufficient financial literacy, and geographical isolation is significant.[61] Regulatory compliance poses an additional considerable obstacle, as authoritative bodies like the Reserve Bank of India and SEBI issue rigorous directives. Ongoing challenges persist in technology integration, especially in light of the advent of critical technologies such as machine learning, blockchain, and artificial intelligence.[62] It is crucial to prioritize the development of trust and consumer loyalty by guaranteeing frictionless transactions, individualized offerings, and intuitive interfaces.[63] It is critical to safeguard consumer data and mitigate cybersecurity threats. Failing to do so exposes consumers to financial vulnerabilities and undermines confidence in the Fintech ecosystem.

Ambiguity in the duty of Data processors: Although the law contains a comprehensive section devoted to data fiduciaries, it fails to adequately address the duties of data processors due to their little liability, as indicated in the PDPDA. The lack of this information is critical since data processors are ultimately accountable for handling the principal's data given to them by the data fiduciaries, subject to the principal's revocable consent. The PDPDA defines the fiduciary and processor's duties and responsibilities as those outlined in a legally enforceable contract, service or outsourcing agreement, or similar instrument.

Overregulation vs. Ease of Doing Business: India's financial services business operates under a comprehensive set of rules that handle concerns related to cyber risk management, consumer protection, data privacy, outsourcing, and

[61] Belli, Luca. "New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance." *Indian JL & Tech. 18, 2022*, p. 145.

[62] Ray, Saon, Sandeep Paul, and Smita Miglani. "Exploring the Regulatory Contexts of Fintech Innovation for Financial Inclusion: The Case of Distributed Ledger Technologies in India." *Artificial Intelligence, Fintech, and Financial Inclusion.* CRC Press, 2023, 39-51.

[63] Marda, Vidushi. "Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making." *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, vol. 376, no. 2133, 2018, pp. 1–19. JSTOR, https://www.jstor.org/stable/26601842. Accessed 21 Mar. 2024.

information security. The adoption of the DPDPA, which addresses data security and privacy issues, has increased regulatory oversight, primarily as fintech and crypto businesses may be classified as Significant Data Fiduciary. The convergence mentioned above necessitates implementing a sophisticated compliance approach, which may be more mature than unregulated peers. Since 2014, these limitations have challenged the government's purpose of encouraging business facilitation.[64]

Product management: Integral to product development processes are the following principles: data security, transparency, and consumer rights. Implementing privacy by design principles, making controls easy to use, creating rules and procedures for data use, and ensuring users' permission is visible are all things to think about.

Risk management: Financial organisations depend significantly on consumer data to evaluate transactional risk, price credit risk, underwrite insurance, and identify fraud.[65] Companies must assess gathered data, seek express customer permission, and demonstrate legal reasons for data acquisition under the DPDPA. The lack of particular data points might impact the efficacy of risk management systems, causing organisations to evaluate tactics and even modify product prices appropriately.

Issue of Consent Mechanism: Effective consent procedures are critical for protecting data privacy and persons' rights. The speed with which people learn these regimens determines their effectiveness. Consent and the 'right to be forgotten' are critical for regulating data storage and dissemination, especially when third-party sharing is for commercial purposes. Standardised, accessible consent processes are essential for consumers to make informed data choices while minimising negative repercussions.

Emerging Technologies: Although not directly regulating them, the DPDPA restricts them. Talks focused on how AI may protect financial data, improve service delivery, personalise services, and ensure transparent data processing. It is decided that more than only consent calls for improved encryption and user approval processes. Furthermore, since the DPDPA focuses more on breaches than damage, it does not define or categorise health data, which is essential for efficient data management. Rules must go beyond security lapses to shield people from possible data abuse. This gap may be filled by reintroducing the Digital Information Security in Healthcare Act 2018 (DISHA).[66] Additionally, laws should change to reflect the rapid spread of cutting-edge technology like wearables, which calls for a unified framework to support industry research, consumer confidence, and regulatory clarity.

Data Localization: There are restrictions on the international transmission of

---

[64] Gugnani, Vidur. "The Companies Amendment Act, 2020: An Initiative towards Ease of Doing Business." *International Journal of Law Management & Humanities*, 4, 2021, pp. 404-418. HeinOnline, https://heinonline-org.elibrary.nirmauni.ac.in/HOL/P?h=hein.journals/ijlmhs9&i=424.

[65] Garg, Hemant. "Financial Regulators and the Need for Data Privacy and Protection-Issues, Opportunities and Challenges." *International Journal of Legal Developments and Allied Issues* 8.1 (2022): 290-301.

[66] Georgiou, Dimitra, and Costas Lambrinoudakis. "Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR)." *Information* 11.12 (2020): 586.

personal data, but it is still possible. Data Fiduciaries may get instructions from the Indian Central Government not to provide personal information to certain foreign countries. To stop cross-border data transfers to countries under restriction, particularly those bordering India, foreign banks must ensure that these directions are followed.[67] Compliance with current regulations—such as the RBI's Data Localization Guidelines—is essential for banks to operate in India. According to these requirements, payment system data may only be maintained inside Indian borders; however, copies can be stored outside for international transactions with permission granted by the DPDPA. Foreign banks may handle transactions remotely from Indian data centres to their global offices, guaranteeing that the data is processed and kept only in India. To comply, data must be deleted from overseas systems and returned to India with the data principal's permission within one business day or 24 hours after processing.

Risk of Research Exemption: The DPDPA does not apply to research, archiving, or statistical processing. Research and analytics from group organisations help international banks improve Indian banking services. These operations are still OK for internal usage as long as they're not used to upsell Data Principals. However, if banks use data access and policies to make customised choices about Data Principals, they need to re-evaluate them.

6. Conclusion

The development of India's fintech industry is mainly dependent on two key factors: data security and privacy. Fintech businesses must continuously use strong data protection policies to ensure the reliability of financial services and to preserve customer trust. Besides legal duties, ethical responsibilities include including a "privacy by design" methodology, adhering to regulatory guidelines, and demonstrating anticipatory awareness of emerging risks. The fintech sector in India should encourage an environment of trust and transparency by prioritising data protection and security, which would make it easier for more people to embrace the advantages of digital financial services. Fintech companies can contribute to creating a strong and ecologically sustainable economic system that propels India towards a bright and inventive future by showcasing a shared commitment to data protection.

An important turning point for the nation will be reached in 2023 with the passage of the PDPDA, which gives people authority over their data. The success of this law depends on a fundamental change in our understanding of privacy and data—a departure from their commodity status. Should this shift in perspective not be accepted, the PDPDA's intended goals may not be achieved.

Financial institutions have a unique chance to improve consumer trust, strengthen data security, and promote responsible data governance thanks to the PDPDA. Financial service companies may become data custodians in an increasingly connected and data-centric world by adopting the PDPDA and navigating changing

[67] Bailey, Rishab, and Smriti Parsheera. "Data localization in India: paradigms and processes." *CSI Transactions on ICT* 9.3 (2021): 137-150.

regulatory regimes. Even while the DPDPA has a global view, it is distinctive in that it requires more than just adhering to international norms to be relevant in the Indian context.

Bibliography

1. Akanfe, Oluwafemi Adeola. *Advancing Digital Financial Inclusion: Data Privacy, Regulatory Compliance, and Cross-Country Cultural Values in Digital Payment Systems Use*. Diss. The University of Texas at San Antonio, 2022.
2. Aldboush, Hassan HH, and Marah Ferdous. "Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust." *International Journal of Financial Studies* 11.3 (2023): 90.
3. Alekseenko, Aleksandr P. "Privacy, Data Protection, and Public Interest Considerations for Fintech." *Global Perspectives in FinTech: Law, Finance and Technology*. Cham: Springer International Publishing, 2022, p. 25-49.
4. Andrae, Silvio. "The role of BigTech in emerging markets." In *Handbook of Banking and Finance in Emerging Markets*, Edward Elgar Publishing, 2022. pp. 433-463.
5. Arner, Douglas W., et al. "FinTech and RegTech: Enabling Innovation While Preserving Financial Stability." *Georgetown Journal of International Affairs*, vol. 18, no. 3, 2017, pp. 47–58. JSTOR, http://www.jstor.org/stable/26395923. Accessed 21 Mar. 2024.
6. Ashta, Arvind, and Guillaume Biot-Paquerot. "FinTech evolution: Strategic value management issues in a fast changing industry." *Strategic Change* 27.4 (2018): 301-311.
7. Bailey, Rishab, and Smriti Parsheera. "Data localization in India: paradigms and processes." *CSI Transactions on ICT* 9.3 (2021): 137-150.
8. Bakare, Seun Solomon, et al. "Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations." *Computer Science & IT Research Journal* 5.3, 2024, p. 528-543.
9. Bali, Vinita. "Data privacy, data piracy: Can India provide adequate protection for electronically transferred data." *Temp. Int'l & Comp. LJ* 21 (2007): 103.
10. Baporikar, Neeta. "Fintech challenges and outlook in India." *Innovative strategies for implementing FinTech in banking*. IGI Global, 2021. 136-153.
11. Bareh, Chanlang Ki. "Reviewing the Privacy Implications of India's Digital Personal Data Protection Act (2023) from Library Contexts." *DESIDOC Journal of Library & Information Technology* 44.1, 2024.
12. Belli, Luca. "New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance." *Indian JL & Tech*. 18, 2022, p. 145.
13. Bhura, Pawan, and Sanjeev Bansal. "Current Status, Trends & Prospects of FinTech in India." *International Journal of Management, Public Policy and Research* 2.4 (2023): 131-138.
14. Bilotta, Nicola, and Simone Romano. *Tech Giants in Banking: The Implications of a New Market Power.* Istituto Affari Internazionali (IAI), 2019. JSTOR, http://www.jstor.org/stable/resrep19672. Accessed 21 Mar. 2024.
15. Bugeja, Diane. "AML/CFT and data privacy regulation: Achieving a peaceful co-existence." *Journal of Financial Compliance* 2.2, 2018, p. 132-141.
16. Chishti, Susanne, and Janos Barberis. *The Fintech book: The financial technology*

handbook for investors, entrepreneurs and visionaries. John Wiley & Sons, 2016.
17. Darbellay, Aline. "Conclusion to Data Governance in AI, FinTech and LegalTech: Law and Regulation in the Financial Sector." *Data Governance in AI, FinTech and LegalTech*. Edward Elgar Publishing, 2022, p. 279-288.
18. Devianti, Dwi Nugrahayu, Prija Djatmika, and Sukarmi Sukarmi. "The Risks Of Personal Data Theft In Fintech-Based Online Loan Applications Due To The Absence Of Law In Indonesia." *Jurisdictie: Jurnal Hukum dan Syariah* 11.2 (2020): 163-181.
19. Dorfleitner, Gregor, Lars Hornuf, and Julia Kreppmeier. "Promise not fulfilled: FinTech, data privacy, and the GDPR." *Electronic Markets* 33.1 (2023): 33.
20. Duraiswami, Dhiraj R. "Privacy and Data Protection in India." *Journal of Law & Cyber Warfare* 6.1 (2017): 166-186.
21. Dutta, Biswadeep. "Bank Licensing in India Defined under Banking Regulation Act 1949: Banking Sectors Journey throughout the Past and the Way Ahead in Future." *Indian JL & Legal Rsch*. 2 (2021): 1.
22. G. Singh, R. Gupta and V. Vatsa, "A Framework for Enhancing Cyber Security in Fintech Applications in India," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 274-279, doi: 10.1109/ICTAI53825.2021.9673277
23. Garg, Hemant. "Financial Regulators and the Need for Data Privacy and Protection-Issues, Opportunities and Challenges." *International Journal of Legal Developments and Allied Issues* 8.1 (2022): 290-301.
24. Goddard, Michelle. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact." *International Journal of Market Research* 59.6 (2017): 703-705.
25. Gomber, Peter, et al. "On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services." *Journal of management information systems* 35.1, 2008, p. 220-265.
26. Gugnani, Vidur. "The Companies Amendment Act, 2020: An Initiative towards Ease of Doing Business." *International Journal of Law Management & Humanities*, 4, 2021, pp. 404-418. HeinOnline, https://heinonline-org.elibrary.nirmauni.ac.in/HOL/P?h=hein.journals/ijlmhs9&i=424.
27. Guha, Dr Shouvik Kumar, Bash Savage-Mansary, and Dr Navyajyoti Samanta. "The Present and Future of AI Usage in the Banking and Financial Decision-Making Processes within the Developing Indian Economy." *Indian Journal of Law and Technology* 18.1, 2022, p. 5.
28. Hernández, Elena, et al. "Data protection on FinTech platforms." *Highlights of Practical Applications of Survivable Agents and Multi-Agent Systems*. The PAAMS Collection: International Workshops of PAAMS 2019, Ávila, Spain, June 26–28, 2019, Proceedings 17. Springer International Publishing, 2019.
29. Hooda, Sneha. "Prevention of Money Laundering Act 2002: An Analysis from Lens of Principles of Law of Evidence." *Issue 5 Int'l JL Mgmt. & Human*. 3 (2020): 997.
30. Jamil, Danish, and Muhammad Numan Ali Khan. "Data protection act in India with compared to the European Union countries." *International Journal of Electrical & Computer Sciences* 11.06 (2011).
31. Kashyap, Amit Kumar, and Mahima Chaudhary. "Cyber security laws and safety in e-commerce in India." *Law & Safety* (2023): 207.
32. Kherala, Hetal. "Financial inclusion: revolution through fintech." *Emerging Trends in International Business and Commerce*, 2019, p. 201.
33. Krishna, Raj. "Data Management in India: A Case Study of Aadhaar Project."

Application of Big Data and Business Analytics. Emerald Publishing Limited, 2020. 127-138.

34. Kukreja, Gagan, Divij Bahl, and Ruchika Gupta. "The impact of Fintech on financial services in India: Past, present, and future trends." *Innovative strategies for implementing Fintech in banking*. IGI Global, 2021. 191-200.
35. Macierzyński, Wiesław Łukasz, and Michał Macierzyński. "Development of new payment services and the role of the fintech sector during the COVID-19 pandemic." *Central European Review of Economics & Finance* 44.3 (2023): 61-78.
36. Marda, Vidushi, and Amber Sinha. "FinTech Lending in India: Taking Stock of Implications for Privacy and Autonomy." *Indian Journal of Law and Technology*, vol. 18, no. 1, 2022, pp. 100-126. HeinOnline, https://heinonline-org.elibrary.nirmauni.ac.in/HOL/P?h=hein.journals/indiajoula18&i=106.
37. Mathew Martin, P. J., and Manukonda Rabindranath. "Digital Inclusion for access to information: A study on banking and financial institutions in India." SAGE Open 7.3 (2017): 2158244017720479.
38. Minto, Andrea, Moritz Voelkerling, and Melanie Wulff. "Separating apples from oranges: Identifying threats to financial stability originating from FinTech." *Capital markets law journal* 12.4 (2017): 428-465.
39. Mohan, N., G. Rajasekar, and Ratno Agriyanto. "Anti-Fraud AI for Banking and FinTech Used in a Proactive Banking Strategy to Thwart SIM Phishing." *The Impact of AI Innovation on Financial Sectors in the Era of Industry 5.0.* IGI Global, 2023. 171-183.
40. Morosanu, Georgiana-Alexandra, Laura Andreea Rata, and Marius Geru. "Aspects Regarding CyberSecurity Developments on SaaS Software Platforms." *EIRP Proceedings* 18.1, 2023, p. 128-146.
41. Murinde, Victor, Efthymios Rizopoulos, and Markos Zachariadis. "The impact of the FinTech revolution on the future of banking: Opportunities and risks." *International review of financial analysis* 81 (2022), p. 102-103.
42. Naithani, Paarth. "Regulating artificial intelligence under data protection law: Challenges and solutions for India." *Indian JL & Just*. 14 (2023): 436.
43. Oyewole, Adedoyin Tolulope, et al. "Data privacy laws and their impact on financial technology companies: a review." *Computer Science & IT Research Journal* 5.3 (2024): 628-650.
44. Pandey, Anoop Kumar. "Introduction to healthcare information privacy and security concerns." *Security and privacy of electronic healthcare records: Concepts, paradigms and solutions* (2019): 17-42.
45. Pandey, Sharad Kumar, and Ravi Dubey. "Critical Analysis of Role of Data Protection in the Growth of FinTech at Global Regime Including India." *Journal of Research Administration* 5.2 (2023): 9538-9553.
46. Prasad M, Deva, and Suchithra Menon C. "The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law." *International Journal of Law and Information Technology* 28.1 (2020): 1-19.
47. Ramkumar, Gowtham. "FinTech in India: A systematic literature review." *The sustainable Fintech revolution: Building a greener future for finance* (2023): 225-250.
48. Ray, Saon, Sandeep Paul, and Smita Miglani. "Exploring the Regulatory Contexts of Fintech Innovation for Financial Inclusion: The Case of Distributed Ledger Technologies in India." *Artificial Intelligence, Fintech, and Financial Inclusion*. CRC Press, 2023, 39-51.
49. Salampasis, Dimitrios, and Anne-Laure Mention. "FinTech: Harnessing innovation

for financial inclusion." *Handbook of blockchain, digital finance, and inclusion*, volume 2. Academic Press, 2018. 451-461.
50. Sastry, V. S. "Indian Insurance Data Issues." Seminar on "Data Base Issues in Financial Sector". 2010.
51. Savitha, Basri, Iqbal Thonse Hawaldar, and Naveen Kumar. "Continuance intentions to use FinTech peer-to-peer payments apps in India.", 2022, *Heliyon* 8.11.
52. Setiawan, Kukuh, and Nadia Maulisa. "The evolution of fintech: a regulatory approach perspective." 3rd International Conference on Law and Governance (ICLAVE 2019). Atlantis Press, 2020.
53. Shehu, Vlona Pollozhani, and Visar Shehu. "Human rights in the technology era–Protection of data rights." *European Journal of Economics, Law and Social Sciences* 7.2 (2023): 1-10.
54. Singh, Gurinder, Ruchika Gupta, and Vidushi Vatsa. "A framework for enhancing cyber security in fintech applications in india." 2021 International Conference on Technological Advancements and Innovations (ICTAI). IEEE, 2021.
55. Stefanelli, Valeria, and Francesco Manta. "The rise of digital finance: empirical evidence on fintech firms, banks and customers." (2022): 1-121.
56. Stewart, Harrison, and Jan Jürjens. "Data security and consumer trust in FinTech innovation in Germany." *Information & Computer Security* 26.1, 2018, p. 109-128.
57. Sundara, Karishma, and Nikhil Narendran. "The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection." *Computer Law Review International* 24.5, 2023, p. 129-141.
58. Thakur, Nikita, and Vandana Sharma. "Enhancing Fintech Security-A Comparative Analysis of Advanced Security Algorithms." 2023 2nd International Conference on Edge Computing and Applications (ICECAA). IEEE, 2023.
59. Tonveronachi, Mario. "Ending laissez-faire finance." Corsi M., Kregel J. e D'Ippoliti C.(a cura di), *Classical Economics Today. Essays in Honor of Alessandro Roncaglia* (2018): 19-32.
60. Walker, George. "International Law: Financial Technology Law: A New Beginning and A New Future." *GP Solo* 34, no. 3, 2017, p. 76-77.
61. Yadav, Yesha. "Fintech and International Financial Regulation." *Vanderbilt Journal of Transnational Law*, vol. 53, no. 3, May 2020, pp. 1109-1146. HeinOnline, https://heinonline-org.elibrary.nirmauni.ac.in/HOL/P?h=hein.journals/vantl53&i=1135.
62. Zhang, Xichen, et al. "Data breach: analysis, countermeasures and challenges." *International Journal of Information and Computer Security* 19.3-4, 2022, p. 402-442.
63. Zheng, Yulu, and Xiaoli Wu. "Fostering fintech innovation: A tripartite evolutionary game analysis of regulatory sandbox experiments." *International Review of Economics & Finance* (2024).