Jurnal Dinamika Hukum

Vol. 24 Issue 1, 2024
E-ISSN 2407-6562 **P-ISSN** 1410-0797
National Accredited Journal, Decree No. 21/E/KPT/2018
DOI: 10.20884/1.jdh.2024.24.1.4074

Fin-tech Regulations Development, Challenges, and Solutions : A Review

Chander Mohan Gupta[1], Gagandeep Kaur[2], Aryuni Yuliantiningsih[3]
Shoolini University, India[1], School of Law, University of Petroleum & Energy Studies, India[2], Universitas Jenderal Soedirman[3]
✉ cg30aug@yahoo.com

Submitted: 24/12/2023
Revised: 24/03/2024; 08/04/2024
Accepted: 19/04/2024

Abstract
Fintech is a term which is the most common and used in the financial sector these days around the globe. Its growth has made it clear that it is there to stay, and it is going to cause a major disruption on the globe level, when talked about in relation to financial markets. It is an old saying, “With great powers come great responsibilities” and the same is true in relation to fintech. With the kind of growth, it is doing it needs to be monitored and regulated on a major level. When we talk about the fast-moving areas where fintech has made an impact are e-invoice, e-payments, deposits, and financial transactions on personal, corporate and government level. When we calculate the scale at which fintech is growing we need to understand that it is just a matter of time that everything will be assessable with a click of a button and if in the wrong hands we can imagine the impact done. When we see the dark side of fintech where the companies have an assesses to the data and every personal information of customers, they can use/misuse the same at their liberty. If we study the cases from around the globe it is a simple practice of which works of a simple rule, “If it works here, it will work everywhere.” This paper also delves into tracing the cyber threats faced by the financial sector due to its reliance on technology and sensitive data. The authors have analysed a number of laws, rules, and guidelines to regulate fintech in India that are designed to foster innovation, protect the interests of consumers, and preserve the country's financial stability. Thus, in the said paper the authors have tried to study the journey of Fintech in relation to its regulatory legal journey, in relation to India.

Keywords: Fintech, Financial Inclusion, Legal Regulations, Legal Issues.

INTRODUCTION

When we think of the sectors that are subject to the highest levels of regulation throughout the globe, the banking industry is the first one that comes to mind. A number of rules, regulations, and laws are in place, and they are responsible for controlling the businesses and the authorities that act in accordance with these laws. The question of why these financial technology businesses are subject to such a high level of regulation continues to be, and the answer is straightforward: "great power comes with great responsibility." Fintech companies are tasked with a large deal of social and financial responsibilities, which is the reason why the government

is more protective of these companies. These limitations apply not just to financial institutions, but also to any sector that provides any kind of financial service over the internet, including fields like insurance and investment for example. Fintech companies, like any other enterprise, face challenges, and the same is true for the finance industry. The regulatory process is conducted in the same manner, and a significant amount of permission from a variety of bodies is required. For the purpose of determining what and when will be given to customers, the company is required to state its goals and territories of operation (Milian et al., 2019). Due to the fact that the journey of Fintech is still relatively young, there has been a significant increase in growth, which has compelled academics, researchers, economists, and regulators to acquire more knowledge about it.

The revolution in technology and the internet, which is considered to be the fourth industrial revolution, has brought about a significant change in industries all over the world. The transformation that has been brought about as a result of the introduction of information technology is something that has not been existent for many decades. According to Xu et al (2018), significant shifts are seen in every aspect of the business, including production, management, and governance. According to Wang et al (2021), the majority of fintech companies consist of startups, and these companies have had an impact on the services sector all over the globe. Starting with PayPal and continuing with razor pay, UPI, BHIM, and barat pe, all of these services are based on the foundation of what is known as sophisticated technology. They have not only caused disruptions in the financial system, but they have also caused customers to switch from an older system to a newer generation of mobile applications. Fintech provides a higher level of financial and economic security to the general public; nevertheless, it also has a shadowy side that has to be watched and cross-checked.

Meaning of Fintech: If we study the World Economic Forum (2015) report which clearly states that avoidance of innovation derived from technology is near to impossible. further stating that technology being the fundamental pillar for the social, cultural, and economic development of society. Hanelt et al (2021) talk about digital transformation to be a continuous process which triggers economic growth, and these changes have led to a new entrant in the market commonly known as Fintech. formulated from the association of finance and technology.

Definition of Fintech: “a definition provided by Financial Stability board (FSB), states," *technologically enabled innovation in financial services that could result in new business models, application, processes or product with an associated material effect on financial markets and institutions and the provision of financial services*" (FSB, 2017b, 2017a). Wherein Organization for economic co-operation and development quotes,*" innovative applications of digital technology for financial services"* (OECD, 2019). Moving further it can also be referred to as “innovators and disruptors in the financial sector that make use of the availability of ubiquitous communication, specifically via the Internet and automated information processing”.

Fintech is a new financial industry that applies technology to improve financial activities (Schueffel, 2016). When we get into the crust it seems simple but when we deep dive into this definition in a sum of traditional banking, plus the use of internet to make the banking work easy and effective. If we get into the history of the fintech it can be traced with the introduction of ATMs in the year 1960's and 1970's. further in the 80's inter personal dial up system was introduced to make the work of the bank effective, and with the growth and usage of internet online banking become possible in 1990s. the journey never stopped here as then came the credit cards and when internet reached the laptops and desktops of individuals it made a positive disruption with the introduction of PayPal. and then came the Apple Pay or Samsung Pay, others are developed by online services companies such as Google Pay or Amazon Pay. Regional initiatives like TWINT (TWINT AG, 2020) in Switzerland these were the international players but soon came the national players as Paytm, BHIM, Phone pe, Bharat pe, Airtel money and not to forget WhatsApp payment options.

When comes to features there are Fintech companies which provide online payment system with privacy rights named GNU Taler, block chain leading to crypto companies can be considered as alternative financial technology. some examples can be Bitcoin, Ethereum etc.

The following table gives a detailed insight on fintech:

S. No	Types	Findings	Sources
1	Payment services	Payments can be both ways (receiving and sending electronically), easy quick and safe making it more convenient Which in turn makes it safe from cash related crimes (Rahman et al., 2020): Services which are covered are: Mobile banking, P2 P payments, E wallet	EY (2017), FSB (2017b, 2017a), World Economic Forum (2017), Subaramaniam et al, (2020), Rahman et al (2020)
2	Credit and lending	increase in online lending and borrowing, platforms working for crowd lending and funding, with an aim of getting small credits by small investors using online platforms.	Morse, (2015), FSB (2017b, 2017a), (Hudon et al. (2019)
3	Insurance services	companies working in this line are called 'Insurtech' it is just giving option for users to choose an insurance by using online options.	IAIS (2018), Chen (2018), S&P (2018) (2018), Deloitte (2018), Stulz (2019)
4	Investment management	Digitally investing in securities, commodities, and assets, which is commonly known as Profolio management when done through the internet, is what is covered under this topic: mobile trading, investment decision making, online brokerage	Zhang & Teo (2014).

After doing a thorough analysis of the existing literature, we have seen that several studies have been conducted in this particular topic. However, upon closer examination of the specific regions in which these studies have been conducted, it

becomes evident that only a limited number of research have been carried out. Furthermore, only a few of these studies have focused on the legal elements related to the subject matter.

RESEARCH PROBLEM

Technology has been there to solve and make things easy for the users, individual or companies or state. With the introduction of technology in the banking sector and the growth of Fintech has not only worked around for the betterment of the whole economy, but there are several loopholes in the system and those lead Financial frauds which leads to have a strigent financial regulation. The main problem which was found in the review of literature that people work around with the companies and show faith but these companies need to be under the scanner and that was the motive behind this article. To understand the legal system taking care of the Fintech issues.

RESEARCH METHODS

The aim main of the said study was to understand the legal framework which has been present in the south Asian country India and how they are trying to tackle the growing need of regulating Fintech. Thus, intensive research was done on the different types of fintech and then the legal provision available to control those. Leading to the final conclusion of this research.

DISCUSSION

1. Contemporary cyber threats in India to fin-tech technology

Fintech technology has been popularized as the next revolution in the technological sector. Fintech is a financial technology system that the companies and the firms are enabling to compete with traditional methods of finance and in the delivery of financial services (Puschmann, 2017). Financial technology on one hand is evolved as a blessing, however, on the other hand it is also creating complex problems in front of legal jurisprudence. The security and safety of a person and his or her data is very much at risk. Though there are laws like General Data Protection Regulation [GDPR] which was created to deal with these kinds of risks however, these laws are governing an entity communicating with Europe (Dorfleitner et al., 2021). Though India is bringing in Digital Personal Data Protection Bill, 2022, however, it is not passed in the Parliament yet. India is trying to create a potential environment for financial technology to boom but there are a number of cyber threats that arise with the emerging financial technology. Some of them are listed below.

a. Data Protection Issue

The financial technology companies collect and process a great amount of data as it is necessary to ship and customise the services accordingly and to meet the market demand. In fintech process, data provided by customers go through a number of gateways while doing a single transaction. There is

no law to govern if there is a violation of privacy during financial transaction. There are laws that deal with violation of privacy in general (Gai et al., 2017). However specifically laws related to financial transactions are in the evolving stage.

b. Cyber Attacks

Presently the technology is evolving every day and hackers have also aware about new modes of hacking into the personal information. Due to lack of sanctions and regulatory framework all these financial technology institutes are the common targets for the cyber attackers or hackers. All these fin tech companies hold a large amount of data that makes them attractive and a vulnerable target for cyber criminals.

c. Distributed Ledger Technology & Smart Contracts

It is an amount of shared and synchronised digital data that is spread across multiple sites and institutions. It does not have a central administrator, or any centralise data storage for example a Blockchain system which can be either public or private (Firouzi et al., 2020). The use of the smart contracts for finance and trade may bring in a number of risks from a legal and practical perspective which are not covered as there is no law to regulate the same.

d. Robotic Process Automation (RPA) & Legal Responsibility

Though the concept of robotic process automation is in discussion, however, there is no regulatory framework to govern it. There is currently a difficulty in identifying the liabilities between the entities involved in the RPA activities so this poses a serious legal risk for the institution that rely on robotic process automation or Robo advisors. If there is a detailed assessment on the functions and operations there must be a number of legal issues involved which are not sanctioned at all (Kalra, 2019).

e. Social Engineering Crimes in the Fintech Sector

Social engineering offenses can have serious negative effects on a person's or an organization's finances, reputation, and legal standing. Social engineering techniques are employed by attackers to manipulate individuals within the organization in order to obtain unauthorized access to systems or confidential data. Stated differently, social engineering crimes entail using psychological manipulation as opposed to technological means to coerce people or organizations into disclosing private information, acting in a certain way, or granting access to resources or systems (Kondratyeva et al., 2021).

f. Cryptojacking in the Fintech Sector

The act of mining cryptocurrency on someone else's computer system without that person's permission is known as "cryptojacking.". Attackers

usually accomplish this by introducing malware intended to mine cryptocurrency onto PCs, servers, or mobile devices. Because cryptocurrencies are becoming more and more popular, hackers might try to use computer resources without the owner's permission in order to mine them, which could negatively affect system performance and result in losses of money. The latest examples of Cryptojacking include Mobile Cryptojacking, cloud based Cryptojacking, Malware based Cryptojacking, fireless Cryptojacking and IoT Device Cryptojacking (Saeed et al., 2022).

g. Phishing Attacks & Malware against Fintech Institutions

Cybercriminals frequently utilize phishing emails, messages, and websites to trick people into disclosing sensitive information, like credit card numbers or login credentials. Infections of fintech devices and systems by ransomware can also lead to data breaches, monetary losses, or service disruptions. Financial institutions in the fintech sector, as well as their clients, are at grave risk from phishing attacks. Smishing (SMS), email phishing, spear phishing, whaling phishing, vishing, credential harvesting, and pharming are a few of the most popular phishing attack types (Despotović et al., 2023).

h. Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks involve flooding a target system, network, or service with a large volume of traffic or requests, rendering it unavailable to legitimate users. Attackers may launch DDoS attacks like User Datagram Protocol (UDP) Flood or Internet Control Message Protocol (ICMP) or NTP (Network Time Protocol) or HTTP flood attack to disrupt fintech services by overwhelming servers or networks with a flood of traffic, rendering them inaccessible to legitimate users (Kaur et al., 2021).

i. Mobile Threats

Mobile devices have become lucrative targets for cybercriminals due to the widespread use of payment apps and mobile banking. Dangers include SIM swapping attacks, phony apps, and mobile malware. Fintech applications and data security may be jeopardized by malicious software designed specifically for mobile devices. Malware for mobile devices can encompass trojans, viruses, and spyware that aim to pilfer confidential data like credit card numbers, login credentials, or personal information kept on the gadget. Financial services servers can listen in on private information being sent over unsecure networks thanks to Man-in-theMiddle (MitM) attacks, which snoop on communication between the mobile device and the servers. The security of fintech apps can be jeopardized and further vulnerabilities exposed when mobile devices are jailbroken (iOS) or rooted (Android) to get around manufacturer restrictions and install unapproved software (Saxena & Nath Tripathi,
2021).

j. Identity Theft

Identity theft fraud is highlighted in this paper by S. Saluja, which was published in the Journal of Financial Crime (2024) as a major vulnerability within the Indian FinTech sector. According to the author, identity theft is the most frequent fraud that FinTech companies in India deal with. The FinTech industry has grown rapidly, especially during the COVID-19 pandemic, and the number of fraud cases has increased at the same time. The study emphasizes how important it is for FinTech companies to create more robust defenses against identity theft and fraud. Even though FinTech companies are the main focus, a quick discussion of how regulators can reduce the risk of identity theft could offer a more comprehensive viewpoint.

Fintech companies face legal and financial ramifications if they disregard regulatory requirements such as cybersecurity regulations, payment card industry standards, and data protection laws. Fintech businesses that provide financial services like lending, investment management, or payments might need to register or apply for licenses from the regulatory bodies in the countries in which they do business. There may be fines, penalties, or legal action if the required licenses or registrations are not obtained. Laws and regulations of consumer protection, which are intended to protect the rights and interests of consumers, are disregarded by fintech companies. Fintech companies involved in financial transactions are subject to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Regulations that are aimed at preventing money laundering, terrorist financing, and other illicit activities (Mahalle et al., 2021).

2. India's fin-tech regulation guarantees to tackle contemporary cybersecurity

The government of India is aware regarding the future of Fin-tech technology as it is going to be a part of our lives. Therefore, taking step towards regulation and control of financial technology in India have also contributed to the growth of this sector. In India following legislations regulate and govern the e-Banking sector and crimes therein:

a. Payment and Settlement Systems Act, 2007

The principal regulation that governs the payment system in India is the Payment and Settlement Systems Act, 2007 (Khurana et al., 2023). In exercise of its powers the PSS Act has been followed by the central bank from time to time and various directions, notifications, and regulations to regulate fin-tech sector in India has been given. As per the Payment and Settlement Systems Act, 2007 any entity which desires to establish or operate a payment system is required to seek specific authorisation of the central bank. PSS Act defines the payment system as a system that enables payment to be affected between a pair and a beneficiary. It has given various regulations and regulatory approaches to govern financial technology in

India. But these have always been on papers and not implemented which is the biggest drawback of the same and because of this financial technology in India still have no law that will govern the financial technology sector of India particularly. Financial technology sector has always been overlapping and a non-linear business model and because of this there is no regulatory framework for fin tech in India so the laws which will be applicable and the rules governing the financial business and technology will depend on the nature of the business that is being conducted.

b. Information and Technology Act, 2000

The IT Act of 2000 is one of the first e-commerce laws enacted by the Indian government. The primary aim of this law was to give ratification to the UNICITRAL model law which is a Law on electronic commerce and was published in 1996. The core objective of the Act was to give legitimacy to the online transactions and finances that are made over the internet and even for transmission of electronic data through electronic methods of communication. The Act further establishes a strong regulatory framework and specifies punishments and penalties as well. Online commerce firms are subject to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011. Section 3 of IT Act deals with authentication of electronic records and section 4 deals with legal recognition of electronic records. Then there is section 10A which deals with validity of contracts that are formed through electronic means. There is another section 43 which deals with penalty and compensation for the damage to computer, computer system etc which deals with a secure access to computer system or computer network and provides for punishment if computer or computer system or computer network is disrupted in an illegal way. There is another section 43A that provides for the compensation for the failure to protect data this section provides for data security and privacy. Section 65 of the information technology Act 2000 deals with tampering with computer source documents in this whoever knowingly or intentionally conceals or destroys or alters or intentionally or knowingly cause any other person to do so will be punishable. Then there is section 66 which deals with computer related offences. 66D is another section that deals with the punishment for cheating by personation by using computer resource and the section that follows it is 66E which provides for punishment for violation of privacy. Section 72 of the act further deals with the penalty for breach of confidentiality, privacy, and section 72A further deals with the punishment for disclosure of information in breach of lawful contract. In total the information Technology act deals with some offences that occurs while using financial technology. IT act is one of the major regulatory frameworks that deals with such offences and provides for punishment as well.

c. Information Technology Amendment Act 2008

Prior to 2008 amendment Act IT Act 2000 had only two sections which dealt with computer related offences generally. The amendment has provided for a stronger data protection measure as well as it has strengthened the further framework against cyber-crimes (Lilian, 2019). There have been a number of issues which were inherent in the nature of the crimes that were evolving from information technology and cyberspace which are solved by the amendment act of 2008 there have been certain specific areas of concerns related to financial technology, Banks and customers and banking sector as a whole which were solved by the amendment act of 2008.

d. Prevention of Money Laundering Act, 2002

Under section 12 of PMLA every banking company, financial institution and intermediary as the case is officially required to maintain a record of transactions as it will be prescribed by the rules and further must provide information to the director within the time limit prescribed. The records shall include the records of cash transactions of more value than ten lakhs or its equivalent in foreign currency, integrally connected cash transactions taking place within a month, cash transactions where forged or counterfeit notes are involved, and suspicious transactions of the nature described therein. These records are to be maintained for a period of 10 years from the date of the transaction when takes place under rule six of prevention of money laundering rules. Prevention of money laundering act in some way or the other governs the financial institutions.

e. Reserve Bank of India, 2021 Guidelines

The financial technology (fintech) sector in India has experienced remarkable growth and significance, evident from the evolution of the fintech department within the Reserve Bank of India (RBI). In 2018, the RBI established a fintech division under the Department of Regulation, which was later moved to the Department of Payment and Settlement Systems in 2020. This department is responsible for regulating fintech activities. To further enhance fintech innovation and address challenges, the RBI has recently created a dedicated Financial Technology Department. This new department will focus on identifying opportunities and forming regulatory mechanisms not only for India but also for the international arena. It will oversee initiatives related to regulatory sandbox and the development of a central bank digital currency. The central bank of India has consistently maintained a customer-centric approach to regulation while striving to keep pace with fintech advancements in the country. To address the dynamic fintech landscape, a working group on digital lending was constituted, which highlighted the growth momentum in digital lending and its implications for financial stability. The group provided recommendations in its report. To support the growth of digital India, the RBI is actively working on developing a robust regulatory framework for the fintech sector. In parallel, the

Indian government has set up a committee to devise a framework for regulating non-personal data. Additionally, the Personal Data Protection Bill 2019, aimed at establishing a comprehensive data protection framework, is currently under consideration by the legislature. Once enacted, this bill will impose stricter data protection obligations on fintech companies and institutions.

f. Digital Personal Data Protection Act, 2023

Significant modifications to data protection and privacy laws are brought about by the DPDP Act 2023 in India, which has affected technology companies, particularly those in the fintech industry that handle sensitive financial data. The Act seeks to improve the protection of personal data by introducing stronger guidelines for data processing. Complying with the DPDP Act 2023 presents a significant challenge for fintech companies, which deal with extremely sensitive financial data. It is imperative that they implement strong data protection protocols to preserve user confidentiality and adhere to the latest regulatory mandates. Serious fines and legal ramifications for noncompliance could make things more difficult for tech companies in the fintech industry. Thus, navigating the changing regulatory landscape while upholding user confidence and trust requires adjusting to the new regulatory framework and putting comprehensive data protection strategies into place.

Growing customer preferences, technological innovation, and favourable regulatory frameworks have all contributed to the fintech industry's explosive expansion in India in recent years. The regulatory environment that oversees this rapidly evolving sector must be examined as fintech companies carry on revolutionizing financial services (Anifa et al., 2022). In order to promote innovation while guaranteeing consumer protection and financial stability, the regulatory bodies in charge of fintech activities in India are discussed in this paper as under:

a. Reserve Bank of India (RBI)

The RBI, which is India's central banking organization, is essential to the oversight and management of the nation's financial sector, which includes fintech operations. Fintech includes peer-to-peer lending, digital banking, payment systems, and cryptocurrency, all of which are regulated by the RBI. Its goals are to reduce systemic risks and preserve financial stability by issuing licenses, establishing regulations, and keeping an eye on compliance. The overarching goals of the RBI in regulating fintech activities are twofold: to mitigate systemic risks and to preserve financial stability. To achieve these objectives, the RBI employs a multifaceted approach that involves the issuance of licenses, the establishment of regulatory frameworks, and the monitoring of compliance within the fintech sector (Ahern, 2020).

Firstly, the RBI is responsible for granting licenses to fintech firms, ensuring that only entities meeting specified criteria are permitted to engage in financial

activities. These licenses serve as a mechanism to uphold standards of professionalism, reliability, and integrity within the industry(Prasad et al., 2019).

Secondly, the RBI sets forth regulations and guidelines governing fintech operations, encompassing aspects such as risk management, data security, and consumer protection. By establishing clear rules and standards, the RBI aims to foster a conducive environment for innovation while safeguarding the interests of stakeholders, including consumers and financial institutions (Rajaiah et al., 2022).

b. Securities and Exchange Board of India (SEBI)

SEBI is the regulatory authority responsible for overseeing the securities market in India. While primarily focused on traditional capital markets, SEBI also regulates aspects of fintech, particularly crowdfunding platforms, roboadvisors, and investment-based fintech solutions. Crowdfunding platforms are one area of fintech regulation that SEBI monitors. These platforms make it easier to raise money for a variety of projects or ventures from a large number of investors. SEBI oversees crowdfunding operations to guarantee investor safety, openness, and adherence to securities regulations (Patel & Patil, 2023). By enforcing investor limits, eligibility requirements, and disclosure requirements for crowdfunding platforms, SEBI aims to protect investor interests and reduce the risks associated with fraudulent schemes. SEBI's mandate includes investor protection, market integrity, and ensuring fair and transparent market practices in the fintech space.

c. Insurance Regulatory and Development Authority of India (IRDAI)

IRDAI regulates the insurance sector in India, ensuring the solvency, integrity, and fair conduct of insurance companies. In the fintech realm, IRDAI oversees insurtech startups and digital insurance platforms, ensuring compliance with regulatory requirements, promoting innovation, and protecting policyholders' interests. Overseeing and regulating digital insurance platforms and insurtech firms is one of the main ways that IRDAI supports the fintech industry. These platforms use technology to offer cutting-edge insurance services and products, like online claim processing, digital insurance plans, and customized insurance options. IRDAI establishes rules and regulations for digital insurance platforms to guarantee consumer safety, openness, and legal compliance.

d. Ministry of Electronics and Information Technology (MeitY)

MeitY is responsible for formulating policies and strategies related to information technology and electronic governance in India. While not exclusively focused on fintech, MeitY plays a crucial role in promoting digital infrastructure, cybersecurity, and data protection, which are integral to the fintech ecosystem. The development of digital infrastructure is one of the main ways that MeitY supports the fintech industry. MeitY is in charge of developing strategies and policies to improve digital accessibility and connectivity throughout the nation.

This includes programs like the Digital India initiative, which seeks to close the digital divide, empower people with digital tools and services, and encourage digital literacy. MeitY fosters an environment that encourages innovation and growth for fintech companies by enhancing digital infrastructure, especially in underserved and remote areas. Additionally, MeitY is essential to maintaining data security and cybersecurity, two things that fintech companies handling private financial data must take very seriously. MeitY creates laws and guidelines pertaining to data privacy, cybersecurity, and encryption standards in order to reduce online risks and protect customer information (Marda & Sinha, 2022).

Therefore, regulatory bodies play a crucial role in shaping the fintech landscape in India. Despite the regulatory framework in place, the fintech sector in India faces several challenges. Regulatory fragmentation, overlapping jurisdictions, and evolving technology pose challenges for both regulators and fintech companies. Moreover, balancing innovation with consumer protection and financial stability remains a constant challenge for regulatory bodies.

CONCLUSION

Technology is here to stay, and it is not always positive. Things can go hay wire if not taken into right direction, and same is the case of fintech. On one side it has given so many advantages that where it has brought the banking and financial services to the palms of the people, but on the other hand it has also taken away their privacy and personal security. People are enjoying the services but on the other hand losing their hard-earned money, and when they reach the law to get remedies for the same what they get is a long road ahead, it not that the law is not present, but the problem is that specific law for specific problems is not available and we have to still rely on the age old legal system. In short, fintech is there to stay but if not controlled in the right direction it can be controllably dangerous.

After analyzing the existing legislative framework, it has been observed that there are so many laws that have become outdated and are not in parallel compliance with the digital world. There is a need for new laws and amendments must be bought in the existing laws for the better regulation of fintech technology.

Thought Fintech is the growing industry and the new norm of payment around the world, but still a lot has to be done in relation to the working of the Firms associated with Fintech. The bigger they grow the more stringent the rules and regulations should be. These giants if not controlled at the right time will be impossible to control if they go wild. Thus, a strong legal system to control the working of these firms is a necessity. Regulating the fintech sector in India requires a balanced approach that fosters innovation while ensuring consumer protection, financial stability, and regulatory compliance. In order to promote experimentation and entrepreneurship in the fintech sector, it is critical to establish innovation hubs, startup accelerators, incubators, and to offer funding, mentorship, and networking opportunities to fintech startups. Furthermore, it is imperative to cultivate innovation, improve regulatory frameworks, advance financial inclusion, and

construct resilient infrastructure in order to fortify the fintech industry in India. Here are some suggestions for effectively regulating the fintech sector in India:

It is important to establish regulatory sandboxes. The creation of regulatory sandboxes under the controlled environments overseen by regulators—that enable fintech companies to test novel goods and services is crucial. While giving regulators the opportunity to evaluate risks and create suitable regulatory frameworks, regulatory sandboxes allow for experimentation that allow fintech companies to test innovative products and services in a controlled environment under the supervision of regulators. Regulatory sandboxes provide a space for experimentation while enabling regulators to assess risks and develop appropriate regulatory frameworks.

It is recommended to implement the concept of proportionate regulation, whereby fintech organizations can customize laws to the unique risks and features of their operations, accounting for elements like scale and complexity. Adopt sensible regulations that balance sufficient risk management and consumer protection with an emphasis on innovation.

Another crucial step for the fintech industry is interagency coordination. In order to fill regulatory gaps and guarantee uniformity in regulatory approaches across various fintech sectors, coordination and collaboration among regulatory agencies, such as 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), may be strengthened.

Financial, reputational, and legal ramifications for individuals and organizations can be severe when it comes to social engineering offenses. Implementing strong authentication procedures, keeping an eye out for common attacks, providing employee training, and utilizing technical controls like email filtering and access controls are all examples of mitigation strategies.

Fintech companies should incorporate strong cybersecurity measures like multifactor authentication (MFA), email authentication protocols (SPF, DKIM, DMARC), employee training and awareness programs, anti-phishing solutions, and regular security audits and assessments to reduce the risk of phishing attacks, mobile threats, and cryptojacking. Sturdy security measures like multifactor authentication, encrypted sensitive data, frequent security updates, user education and awareness campaigns, and real-time mobile transaction monitoring for questionable activity are all important for fintech companies to have.

To manage regulatory compliance risks effectively, fintech companies should establish robust compliance programs, conduct regular compliance assessments and audits, invest in compliance technology and automation tools, and maintain open communication with regulatory authorities. It is relevant to provide clear regulatory guidance, standards, and best practices for fintech companies to promote

compliance with regulatory requirements and enhance transparency and accountability.

REFERENCES

Ahern, D. M. (2020). Regulators Nurturing FinTech Innovation: Global Evolution of the Regulatory Sandbox as Opportunity Based Regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3552015

Anifa, M., Ramakrishnan, S., Joghee, S., Kabiraj, S., & Bishnoi, M. M. (2022). Fintech Innovations in the Financial Service Industry. *Journal of Risk and Financial Management*. https://doi.org/10.3390/jrfm15070287

Chen, C. C. (2018). Regulatory Sandbox and InsurTech: A Preliminary Survey in Selected Countries. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3275929

Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In *Contributions to Finance and Accounting*. https://doi.org/10.1007/978-3-031-23269-5_15

Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2021). Promise Not Fulfilled: Fintech Data Privacy, and the GDPR. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3950094

EY.ai. (2017). *Global FinTech Adoption Index 2017*. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/bankingand-capital-markets/ey-fintech-adoption-index-2017.pdf

Financial Stability Board. (2017a). *Financial Stability Implications from FinTech*. https://www.fsb.org/2017/06/financial-stability-implications-from-fintech/

Financial Stability Board. (2017b). *FinTech Credit: Market Structure, Business Models and Financial Stability Implications*. https://www.fsb.org/2017/05/fintech-credit-market-structure-businessmodels-and-financial-stability-implications/

Firouzi, F., Chakrabarty, K., & Nassif, S. (2020). Intelligent Internet of Things: From Device to Fog and Cloud. In *Intelligent Internet of Things: From Device to Fog and Cloud*. https://doi.org/10.1007/978-3-030-30367-9

Gai, K., Qiu, M., Sun, X., & Zhao, H. (2017). Security and privacy issues: A survey on fintech. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-319-52015-5_24

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change. *Journal of Management Studies*. https://doi.org/10.1111/joms.12639

Hudon, M., Labie, M., & Szafarz, A. (2019). A long time ago in a galaxy far, far away ... How microfinance evolved and how research followed. In *A Research Agenda for Financial Inclusion and Microfinance*. https://doi.org/10.4337/9781788114226.00007

International Association of Insurance Supervisors. (2018). *ssues Paper on the Increasing Use of Digital Technology in Insurance and its Potential Impact on*

Consumer Outcomes. https://www.iaisweb.org/uploads/2022/01/180801Issues-Paper-on-the-Increasing-Use-of-Digital-Technology-in-Ins-its-Potential-Impact-on-Consumer-Outcomes.pdf

Kalra, D. (2019). Overriding FINTECH. *Proceeding of 2019 International Conference on Digitization: Landscaping Artificial Intelligence, ICD 2019*. https://doi.org/10.1109/ICD47981.2019.9105915

Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends. In *Springer*.

Khurana, A., Kumar, A., & Jain, M. (2023). *Fintech Laws and Regulations India 2023-2024*. The International Comparative Legal Guides and the International Business. https://iclg.com/practice-areas/fintech-laws-andregulations/india

Kondratyeva, M. N., Svirina, D. D., & Tsvetkov, A. I. (2021). The role of information technologies in ensuring banking security. *IOP Conference Series: Materials Science and Engineering*. https://doi.org/10.1088/1757899X/1047/1/012069

Lilian, E. (Ed.). (2019). *Law, Policy and the Internet*. Hart Publishing.

Mahalle, A., Yong, J., & Tao, X. (2021). Regulatory Challenges and Mitigation for Account Services Offered by FinTech. *Proceedings of the 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2021*. https://doi.org/10.1109/CSCWD49262.2021.9437631

Marda, V., & Sinha, A. (2022). FinTech Lending in India: Taking Stock of Implications for Privacy and Autonomy. *Indian Journal of Law and Technology*, *18*(1). https://www.ijlt.in/journal/fintech-lending-in-india%3Ataking-stock-of-implications-for-privacy-and-autonomy

Milian, E. Z., Spinola, M. de M., & Carvalho, M. M. d. (2019). Fintechs: A literature review and research agenda. *Electronic Commerce Research and Applications*. https://doi.org/10.1016/j.elerap.2019.100833

Morse, A. (2015). Peer-to-Peer Crowdfunding: Information and the Potential for Disruption in Consumer Lending. *Annual Review of Financial Economics*. https://doi.org/10.1146/annurev-financial-111914-041939

Patel, P., & Patil, S. (2023). Embracing Fintech: India's progress in the digitalization of the financial industry. *Prayukti – Journal of Management Applications*. https://doi.org/10.52814/pjma.2023.3203

Prasad, A. S., Raghavan, M., Chugh, B., & Singh, A. (2019). *Implementing the Personal Data Protection Bill : Mapping Points of Action for Central Government and the future Data Protection Authority in India*. *October*.

Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering*, *59*(1), 69–76. https://doi.org/10.1007/s12599-017-0464-6

Rahman, M., Ismail, I., & Bahri, S. (2020). Analysing consumer adoption of cashless payment in Malaysia. *Digital Business*. https://doi.org/10.1016/j.digbus.2021.100004

Rajaiah, J., Majumder, A., Ingale, K., & Pasumarti, S. S. (2022). Central Bank and Fintech: Regulatory Challenges and Framework. In *Contributions to Finance and Accounting*. https://doi.org/10.1007/978-3-031-11545-5_3

S&P Global Market Intelligence. (2018). *2018 US Fintech Market Report*. https://www.spglobal.com/marketintelligence/en/documents/2018-usfintech-market-report.pdf

Saeed, S., Almuhaideb, A. M., Kumar, N., Zaman, N., & Zikria, Y. Bin. (2022). Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications. In *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*. https://doi.org/10.4018/978-1-6684-5284-4

Saxena, A., & Nath Tripathi, S. (2021). Exploring the Security Risks and Safety Measures of Mobile Payments in Fintech Environment in India. *International Journal of Management (IJM)*.

Schueffel, P. (2016). Taming the beast: A scientific definition of fintech. In *Journal of Innovation Management*. https://doi.org/10.24840/2183-0606_004.004_0004

Stulz, R. M. (2019). FinTech, BigTech, and the Future of Banks. *Journal of Applied Corporate Finance*. https://doi.org/10.1111/jacf.12378

Subaramaniam, K., Kolandaisamy, R., Jalil, A. Bin, & Kolandaisamy, I. (2020). The impact of E-Wallets for current generation. *Journal of Advanced Research in Dynamical and Control Systems*. https://doi.org/10.5373/JARDCS/V12SP1/20201126

The Organisation for Economic Co-operation and Development. (2019). *Financial Markets, Insurance and Pensions: Inclusiveness and Finance*. https://www.oecd.org/finance/Financial-markets-insurance-pensionsinclusiveness-and-finance.pdf

Wang, Y., Xiuping, S., & Zhang, Q. (2021). Can fintech improve the efficiency of commercial banks? —An analysis based on big data. *Research in International Business and Finance*. https://doi.org/10.1016/j.ribaf.2020.101338

World Economic Forum. (2017). *Beyond Fintech: A Pragmatic Assessment Of Disruptive Potential In Financial Services*. https://www3.weforum.org/docs/Beyond_Fintech_-_A_Pragmatic_Assessment_of_Disruptive_Potential_in_Financial_Services.pdf

Xu, M., David, J. M., & Kim, S. H. (2018). The fourth industrial revolution: Opportunities and challenges. *International Journal of Financial Research*. https://doi.org/10.5430/ijfr.v9n2p90

Zhang, Z., & Teo, H. H. (2014). The impact of mobile trading technology on individual investors' trading behaviors: The "two-edged sword" effect. *ECIS 2014 Proceedings - 22nd European Conference on Information Systems*.