E-ISSN-2583-1208

VOLUME 3|
ISSUE 2| 2023

DAMODARAM SANJIVAYYA NATIONAL LAW UNIVERSITY

DSNLU JOURNAL OF SCIENCE, TECHNOLOGY AND LAW

Center for Intellectual Property Rights & Technology, DSNLU.

ADVISORY BOARD

CHIEF PATRON

PATRON

EDITOR IN-CHIEF

EDITOR

FACULTY EDITORIAL BOARD

STUDENT EDITORIAL BOARD

Information and Disclaimer

Published by the Registrar

DAMODARAM SANJIVAYYA NATIONAL LAW UNIVERSITY

Citation for the Volume – 3 (2) DSNLU J. SCI. TECH. L. (2023)

FOREWORD

The Center for Intellectual Property Rights & Technology (CIPR&T) was established in 2017 with the motive to provide effective research and policy inputs in the field of IPRs and technology. It is the endeavor of the CIPR&T to become the beacon in the field of Intellectual Property Rights and Technology Law by encouraging synthesis of knowledge and best practices cutting across academia, practitioners and research fraternity. CIPR&T publishes a journal to promote scholarly discourse and research in the field of intellectual property law. This process involves curating a collection of academic articles, research papers, and case studies written by experts, practitioners, and students. The journal aims to address current developments, challenges, and innovations in IPR, fostering a deeper understanding of its implications on industries, legal systems, and society. By providing a platform for such contributions, the Centre contributes to the growth of IPR scholarship and helps shape the future of intellectual property policy and practice.

It is with great pleasure that CIPR&T presents the latest edition of the journal, themed "Fintech and Intellectual Property Rights." In this rapidly evolving digital age, the intersection of financial technology and intellectual property has become increasingly relevant, sparking vital discussions that shape the future of both industries. Fintech, with its disruptive innovations, has transformed the way financial services are delivered, making transactions faster, more efficient, and accessible to a broader audience. From blockchain to artificial intelligence, fintech innovations challenge traditional business models, paving the way for new legal and regulatory frameworks. At the heart of this technological revolution is intellectual property, which not only safeguards the innovations driving fintech but also provides the foundation for sustainable growth and competitiveness in this dynamic sector.

This issue 2 of vol 3 explores the synergy between IPR and Fintech, drawing insights from professionals, research scholars and students. Through a series of thought-provoking articles, research papers, and case studies, it aimed to shed light on the complex relationship between fintech and intellectual property rights, offering new perspectives and actionable solutions for practitioners, academics, and policymakers alike.

As Albert Einstein once said, "The mind that opens to a new idea never returns to its original size." The objective of the journal is not only to enrich the academic and legal communities but also to inspire innovative thought and solutions in the evolving domain of IPR. This journal stands as a testament to the Centre's unwavering commitment to fostering intellectual property research. I sincerely thank the editorial team and all the contributing authors for their invaluable efforts in bringing this edition to life. Their contributions have enriched the discourse on fintech and intellectual property rights, and I am confident they will inspire further innovation in this field.

Prof. D. Surya Prakasa Rao
Hon'ble Vice chancellor, DSNLU

FOREWORD

We are delighted to present Issue 2, Volume 3 of the Journal of Science Technology and Science, themed "Evolution of Law and Technology in Financial Markets in India." This edition arrives at a pivotal moment, reflecting the transformative intersection of law, technology, and finance in India's financial landscape. Contributions from PhD scholars, academicians, and law students across the nation provide deep insights into topics like regulatory sandboxes for fintech, the payment industry, and prepaid payment instruments, highlighting their roles in fostering innovation while ensuring compliance.

This issue covers essential topics, including developing regulatory frameworks for Buy Now Pay Later (BNPL) services to enhance financial inclusion. The rise of artificial intelligence in corporate law is comprehensively reviewed, alongside analyses of technology company acquisitions and strategies for a balanced regulatory approach to fintech. Additionally, the importance of data protection and cybersecurity is underscored, particularly their impact on mergers and acquisitions and the legal ramifications of AI-generated content concerning copyright, ownership, and fair use. We also delve into the significance of regulatory sandboxes and bodies in India, the legal challenges of Central Bank Digital Currencies (CBDCs) and smart contracts, and the Reserve Bank of India's regulatory dilemmas regarding digital lending. The interdisciplinary approach to data localization and financial data protection in fintech, legal safeguards in digital banking, and the complex relationship between cloud technology, law, and future advancements are explored. Blockchain's potential to revolutionize contract law and the non-traditional criminalization of virtual crimes in the age of artificial intelligence are also key topics.

We extend our heartfelt gratitude to the authors for their invaluable contributions and unwavering commitment to presenting their work. Your dedication has enriched this edition with high-quality scholarly insights. We also thank our reviewers for their meticulous analysis and valuable comments, which have been instrumental in refining these papers. We hope this edition inspires further research and dialogue on these transformative issues.

Dr. Dayananda Murthy C.P,
Faculty Convenor,
DPIIT-IPR Chair, DSNLU,
CIPR&T, DSNLU

Index

Pg No.

Short Articles

Long Articles

OPENING THE PANDORA'S BOX WITH CBDC: A QUESTION OF LEGALITY & ENFORCEABILITY OF SMART CONTRACTS IN INDIA

- *Disha Mazumdar*[1]

Abstract

RBI's decision to launch Central Bank Digital Currency (CBDC) by undertaking pilot projects with eight other banks propelled the debate on the legality of smart contracts. The RBI's concept notes on CBDC explained its use but it failed miserably to acknowledge the question of the legality of smart contracts in India. The concept of CBDC nudges towards the use of blockchain technology in India especially in the finance sector. Such a paradigm shift would not just introduce the concept of partial decentralization in banking but would also curtail the unnecessary involvement of multiple third parties in the banking system. RBI's gamble to use CBDC puts a question mark regarding the legality and enforceability of smart contracts in India. The paper explains how smart contracts are perfect contracts under the Indian Contract Act, 1872 and how courts apply the legal and economic principles to interpret the enforceability of such contracts. The paper further concludes with suggestions which could be used by the stakeholders to build a robust banking mechanism.

Keywords: *Smart Contracts, CBDC, Blockchain Technology, Nick Szabo, Decentralized Ledger Technology.*

[1] PhD Scholar, Gujarat National Law University. Gmail: disha03101996@gmail.com

I. Introduction

The banking industry in India always tries to keep pace with the evolution of technology. Not only did it revolutionize the payment system from offline to digital it also implemented the ease of UPI[2] (Unified Payments Interface). The main intention of having a cashless economy was to decrease the cost and the tedious task of managing cash. Physical cash demanded the expenditure of printing and its management. The Reserve Bank of India in its report estimated that four crores were spent in 2021 on cash management[3] which only included social and governance costs. Such costs fall on the shoulders of the general public, business enterprises, banks and the RBI. With Central Bank Digital Currency (CBDC) the management, transportation printing and replacement[4] cost of notes would be curtailed. The decision to execute such pilot projects paves the pathway for the acceptance of smart contracts in the financial sector. Such currency would be based on the distributed ledger technology which makes the process decentralised along with having the authentication of RBI to transact such currency.

CBDC is a programmable currency that could be used for a predefined purpose. This feature of programmability gives the ultimate power to decide the feature of CBDC. Such currency paves a pathway for blockchain technology in the financial sector. Apart from being used for smart contracts, blockchain has multiple benefits which could maximize the financial utility.

Although the implementation of a programable currency looks very lucrative on the surface it raises huge doubts about the enforceability and legality of such contracts.

The paper explains the concept of smart contracts and what makes them smart from traditional contracts. This relates the evolution of blockchain through the vision of Satoshi Nakamoto and Nick Szabo and how it adopted the concept of a decentralised Internet. It draws attention towards RBI's new creativity of digital currency through CBDC and how it carries the features of blockchain technology to transact digital currency. The paper compares smart contracts with traditional contracts and argues why smart contracts are perfect contracts under the Indian

[2]RESERVE BANK OF INDIA, MASTER CIRCULAR, *Discussion Paper on Charges in Payment Systems, (*Aug. 17, 2022) *https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=21082#10*(last visited Sept. 21, 2023).
[3]The Pioneer, *Digital currency to cut RBI's cash management costs, drive financial inclusion*, DAILY PIONEER (Nov. 6, 2022), https://www.dailypioneer.com/2022/business/digital-currency-to-cut-rbi-s-cash-management-costs.
[4]MINISTRY OF FINANCE, PRESS RELEASE (Dec. 12, 2022), https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883 (last visited Sept. 20, 2023).

Contract Act, 1876. The author concludes the paper by suggesting how smart contracts and blockchain should not be just limited to CBDC and can be used optimally by banks to revolutionise the financial sector.

II. The "Smart" Contracts

To understand the mosaic, it is essential to study the components which form the mosaic. The term smart contract is not a recent contribution to the world, rather the concept has been existing in the world for a long time. The best example of a smart contract can be the vending machine which supplies us with coffee or tea.[5] Once the coin is inserted, the options are selected; the machine gives an output which can be tea or coffee.

The term smart contract was defined by American cryptographer and coder Nick Szabo.[6] He stated smart contracts are self-executing contracts with the use of computer codes and rules. Now these contracts are deployed on the blockchain and operate according to it. In most common words we can say that such contracts are software programs that are autonomous and bring out specific results. Such results can be the transfer of digital currency (cryptocurrency) through blockchain.

The best example of a smart contract transaction is between an employer and an employee. The employer would transfer cryptocurrency at the end of the month as salary only if the employee fulfills his condition of uploading the documents in the company portal. Here the employer and the employee themselves would not indulge in the contract execution rather the smart contract would execute on its own. The cryptocurrency from the account of the employer would get transferred only if the portal has the documents. Now this contract is based on if/then statements[7] which are coded in computer language and not human language. Hence it can be easily executed without human interference. This is the absolute reason that smart contracts are called self-enforcing contracts making them 'smart' in reality.

[5] Gregory Klass, *How to Interpret A Vending Machine: Smart Contracts And Contract Law*, 7 GEO. L. TECH. REV. 69 (2023).
[6] Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY 9 (1997).
[7] Nataliia Filatova, *Smart Contracts from the Contract Law Perspective: Outlining New Regulative Strategies*, 28 IJLIT 217 (2020).

III. What is Blockchain Technology?

Smart contracts can be either based on singular existence (vending machines) or can be based on blockchain technology. The earlier concept is a bit older and is of not much use in the present tech-driven society. The paper is based on the use of smart contracts installed on the blockchain. To understand blockchain technology we have to understand the history behind the same.

1. Nick Szabo's Objectives

The definition of smart contracts looked very lucrative but the possibility of their existing within the paper was much easier than being a reality. Nick Szabo studied the concept of smart contracts based on two fundamentals. Firstly, he knew people wanted to reduce the cost of transactions due to the presence of the middleman. Secondly, the smart contracts were digital making the process smoother and transparent.[8] He wanted to formulate cryptocurrencies and was working on the same.

Blockchain technology was one of the most significant developments in the world. The financial crisis in the year 2008 which shook the market across the globe, was one of the triggers to develop a decentralized technology.[9] Blockchain technology was used for the first time for Bitcoins when an anonymous group by the name of Satoshi Nakamoto released a white paper on Bitcoin: A Peer-to-Peer Cash System.[10] The paper elaborated on the idea of peer-to-peer[11] money transfer without any intermediary. The paper applied the concept of Nick Szabo to transact digital currency and store it in a digital ledger.[12] This created the platform for implementing smart contracts. As the contract is based on computer codes, the computer would[13] follow a specific set of rules to reduce the transaction cost. Now blockchain consists of two terms: block

[8] Aditi Vinzanekar& Shashank Venkat, *Decentralising the Internet: The Technicality and Legality Behind Smart Contracts*, 32 RSRR (2018).
[9] Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, 2014, E.D. Tex, No. 4:13-CV-416.
[10] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, United NATION SENTENCING COMMISSION (2009),https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf (last visited Sept. 5, 2023).
[11] 16 IMRAN BASHIR, MASTERING BLOCKCHAIN: DISTRIBUTED LEDGER TECHNOLOGY, DECENTRALIZATION AND SMART CONTRACTS EXPLAINED, (2nd ed. 2018).
[12] Max Raskin, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 FORDHAM J. CORP. & FIN. L. (2015).
[13]Jelena Madir, *Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?* SSRN(Dec. 14, 2018), https://deliverypdf.ssrn.com/delivery (last visited Sept. 15, 2023).

and chain. It refers to blocks/packets that are linked to one another through cryptographic function and are used to store data just like a digital ledger.

2. Proof of Work

Blockchain gained its popularity from the concept of verification which helped to maintain its authenticity. Every block on the chain would have data and the address of the block would have the hash function of the previous block to maintain continuity. Blockchain networks have nodes[14] which are the computers themselves, which verify the transaction after every step. Through the nodes participating in the network, there is an agreement entered between the parties which acts as a consensus mechanism in the blockchain. This agreement is an essential point to be explored as all the parties agree to the terms and conditions of the blockchain. Further, the transactions are also viewed and verified according to the PoW (Proof of Work).[15]

The blockchain is a dispersed or distributed network and every party to the blockchain has the complete details of all the transactions. Blockchain technology is highly stable. Every step which takes place is recorded in the blocks and it is extremely difficult to make any alteration and is directly notified to all the users in the blockchain. It is just like a shared Google document where only the parties who have access to it can make changes and the others have viewing rights. It helps to validate the transaction making it highly secured in nature.

3. Web 3.0 and Decentralisation

Smart contracts do not always need blockchain technology to function; it depends on how they have been coded by the parties. Some smart contracts run on the decentralised ledger technology; they are not controlled by any third party. This is one of the essential features of Web 3.0. The evolution of the Internet went through a significant change over the period.[16]

The era of the internet began with Web 1.0 which was static and monotonous. Interaction was not an option available to users. Encyclopedia is the best example where the information could only be read by the users and nothing could be written back. Web 2.0 changed the structure of

[14]The World Bank, *Distributed Ledger Technology (DLT) and blockchain*,(2017), http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-DistributedLedger-Technology-and-Blockchain-Fintech-Notes.pdf

[15]*Id.*

[16] MASSIMO RAGNEDDA&SIUSEPPE DESTEFANIS, BLOCKCHAIN AND WEB 3.0: SOCIAL, ECONOMIC AND TECHNOLOGICAL CHALLENGES 175 (2019).

interaction between users and allowed the sharing of information and giving feedback for any information on the internet.[17] Wikipedia was the trend during this period where users could read and write information on the internet. The Internet was no longer static and monotonous which pushed the development of social media platforms.

Web 3.0 was the third stage of development which introduced blockchain technology into the world. The internet which was earlier controlled and dominated by private entities and governments across the globe was now shifting towards decentralization. The main purpose of the technology was to cut the third-party intermediary and save the cost which was earlier incurred by the middleman. The reason blockchain technology is presumed to be a revolution in Web 3.0 is because of its unique features of decentralisation along with high stability.

The earlier part of the paper explained the concept of smart contracts and how they use blockchain technology for functioning. Now CBDC is an amalgamation of smart contracts and blockchain technology and the next part of the paper explains in detail this amalgamation. CBDC is not a cryptocurrency which operates on blockchain rather is a type of digital currency which is RBI's legal tender.

IV. Let's Talk Revolution

The idea of CBDC was given by an American economist James Tobin.[18] He stated that the Federal Reserve Banks in America could build an alternative which would work exactly like currency but would be more secure. CBDCs are a digital currency which has all the features of a fiat currency and is the liability of the Central Bank.[19] Central Banks of different countries tried to analyze the functioning of CBDC and the future opportunities associated with it. The Union Budget 2022-23 in India stipulated the use of blockchain technology along with a hybrid mechanism to reduce the cost incurred by the banks and make the process more efficient. Even the Reserve Bank of India Act, of 1934 was amended to include digital currency[20] under the act

[17] *Id.* at 5.
[18] Fernando Morera, *Central Bank Digital Currencies- Recent Transatlantic Developments*, WORDPRESS (Apr. 16, 2021), https://ttlfnews.wordpress.com/2021/04/16/central-bank-digital-currencies-recent-transatlantic-developments/
[19] T Rabi Sankar, *Panel Discussion on, 'Central Bank Digital Currencies: Is This the Future of Money?'*, VIDHI CENTRE FOR LEGAL POLICY (Jul. 22, 2021), https://vidhilegalpolicy.in/events/panel-discussion-on-central-bank-digital-currencies-is-this-the-future-of-money/
[20] RESERVE BANK OF INDIA, CONCEPT NOTE ON CENTRAL BANK DIGITAL CURRENCY, (Oct. 7, 2022), https://www.rbi.org.in/Scripts/PublicationReportDetails (last visited Sept. 19, 2023).

and allowed the implementation of pilot projects. Smart contracts do not constitute the whole aspect of CBDC rather they would be used to program CBDC. What makes CBDC unique is that it is a legal tender which supports Distributed Ledger Technology (DLT) and is programmable in nature.

1. Legal Tender

The CMPI-MC Report which was published in 2018[21] stated that CBDC is a central bank currency in digital form. Hence, the central bank would be the issuer and incur the liability for it. It could be used as a medium of exchange or a store of value. It is a sovereign currency which is a legal tender and can be exchanged in the place of fiat currency. CBDC would be the liability of the Reserve Bank of India and the commercial banks would not maintain any transactional details for it. CBDC is a two-way street, which not only aids the bank in reducing the transactional cost, but it also helps to protect the consumers from the craze of cryptocurrency transactions. CBDC being a legal tender gives the autonomy to trade in digital currency with a safety net. Now in case the consumers want to trade in fiat currency they can change the e-rupee to fiat currency and make the transaction. The purpose of digital currency is not to eliminate UPI rather it is to be complimentary.

2. Distributed Ledger Technology

The pilot project tries to experiment with the technology which is to be used for the CBDC which has also been mentioned in the concept note of RBI. The banks have two options one using the traditional centralised technology and the other using the DLT. Now DLT works on the principle of consensus and makes it easier for the parties to give their consensus for every transaction on the blockchain. Although, the infrastructure for fully digital ledger technology is yet to be developed by the country a hybrid alternative would be the most suitable option. It offers higher security and better protection from cyber frauds it gives the process a decentralized touch by reducing the middleman.

3. Programmability[22]

[21] Committee on Payments and Market Infrastructure, Central Bank Digital Currencies, 7-9 (Mar. 12, 2018), https://www.bis.org/cpmi/publ/d174.html.

[22]Patrick McConnell, *CBDC-How Dangerous is Programmability*, THE FENRIG BLOG (Sept. 21, 2021), https://sites.duke.edu/thefinregblog/2021/09/21/cbdc-how-dangerous-is-programmability/

Not much sense can be derived if we say our money can be programmable. The term programmable money was not defined for a long time and there was a lot of ambiguity. Alexander Lee of the Federal Reserve[23] differentiated between programmable money and programmability as programmable money is a digital form of money but programmability of money is a behaviour of money which can be pre-decided by computer codes. Banks can regulate the way money is being used due to the previous codes. However, such a process can only happen when there is a contract between the consumer and the bank. All of which follow the legal terms, banking terminologies and consumer rights. In case of failure on the part of the bank actions will be taken and restitution can be claimed. This is the exact mechanism of smart contracts. The difference is that electronic money and computer codes are stored on the same block/ network. This code is written in a special language called solidity which participants could read. But no alteration could be made to this code which makes the smart contracts immutable unless it has a self-destruct option coded in it.

The use of smart contracts may be a grand move but the question of the legality of such contracts needs to be settled. Cases of failure of payments through CBDC or technical problems incurred in CBDC transactions could lead to the question of the legality and enforceability of such contracts.

V. Smart Contract vs. Traditional Contract

Under English law, the status of smart contracts has been debated for a long time. UK Jurisdiction Taskforce (hereinafter UKJT) is a technology-based legal setup that published its legal statement to answer the questions on cryptocurrency and smart contracts under the common law. The report states automaticity is the feature relating to smart contracts without human intervention. But there would always be a situation where the performance of the parties is affected due to some external forces which are outside the control of the codes which would lead to adjudication by the courts. Under the common law, contracts need not be in a specific way rather they should have three segments which should be fulfilled by the parties. First, the agreement between the parties should be certain and not ambiguous. Second, the parties should

[23]Alexander Lee, *What is Programable Money?* , FEDERAL RESERVE (June 2021), https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money (last visited Sept. 20, 2023).

have an intention to fulfil the agreement. Third, there has to be something beneficial for both parties i.e., consideration.[24] Any contract which satisfies these three criteria is sufficient to be governed by English law.

In cases when the courts have to interpret the contract, they analyse the intention of the parties who decided to get into an agreement. This is done through the language of the contract. Interpretation of modern contracts depends on the language. Unless there is a situation of ambiguity, courts would interpret the surface meaning of the contracts. Generally, the smart contracts are in code language which is different from the natural language. Hence smart contracts are clear as it is devoid of multiple interpretations. So, when the English courts interpret such contracts, they just have to interpret the codes of the contract. So smart contracts are not devoid of general interpretation under the traditional contract law.

In some cases, smart contracts would have ambiguities in the code in those situations the code would be insufficient to ascertain the contractual intention between the parties. In such a situation, the judge would have to look beyond the general interpretation of the code where the external evidence would have a role to play. The judges would have to analyse the circumstances of the contract, the intention of the parties and the intention behind the drafting of the codes.[25] The legislative structures of common law countries are similar.[26] Indian Contract Act, 1876 which has derived its roots from the English law would have the same legislative requirements.

1. Legality of Smart Contracts

It is easy to debate that smart contracts have no relation to traditional contracts and are drastically different. But in reality, there is more similarity between them. The UNCITRAL Model Law places smart contracts in the same parlance as e-contracts. Now e-contracts are just traditional paper written contracts which are converted into digital form for the parties to perform. Smart contracts took a further leap in technology with the essence of blockchain and the implementation of cryptocurrency.[27]

[24] UK Jurisdiction Taskforce, Legal Statement on Crypto assets and Smart Contracts (2019).
[25] *Id.*
[26] Deepti Pandey & Harishankar Raghunath, *Stationing Smart Contract as a 'Contract': A Case for Interpretative Reform of the Indian Contract Act,1872*, 13 NUJS L.REV 4 (2020).
[27] *Id.*at 9.

Although, traditional contracts are more focused on ex-post-performance, smart contracts are based on ex-ante performance. The interpretation clause[28] under the Indian Contract Act defines what an agreement is. The term agreement[29] states that an agreement constitutes multiple promises or sets of promises which would act as a consideration for each other. Smart contracts are sets of promises which are in digital format which include certain protocols and depend on which the parties perform their obligation.[30] So smart contracts follow the same principle of proposal, consideration, acceptance and agreement. Now such an agreement to be enforceable has to qualify the grounds stipulated under section 10[31] of the Act.

Now all the smart agreements which are entered between the parties would not constitute a contract under law. To become a contract, it has to be enforceable under the law. Now the definition of contract under section 2(h)[32] of the Act is very inclusive, which states that all agreements under the sun which could be enforceable under the law would become a contract. Now this enforceability has to be tested on the grounds given under section 10[33] of the Act. We need to understand the wording of section 10[34] which comprehensively states all agreements would become a contract if they are made by the free will of the parties who are not a minor and are competent to contract under the law. The contract made should be for a lawful object and have lawful consideration. Any such agreement should not be expressly barred under the law. To become a contract, the smart contract must satisfy the above-written criteria.

By default, smart contracts are computer codes which run on if-then statements. It becomes extremely easy for the computer to verify whether the above criteria under the law have been fulfilled or not. Smart contracts cannot be altered easily hence, the parties are extra cautious while drafting such contracts and they are accompanied by experts who draft the contract for them. So just like traditional contracts if smart contracts accomplish the grounds under section 10, they form a legal contract under the Act. But what about its enforcement? Are smart contracts self-enforcing in nature?

[28] The Indian Contract Act, § 2 (1872).
[29] The Indian Contract Act, § 2(e) (1872).
[30] NICK SZABO, SMART CONTRACTS: BUILDING BLOCKS FOR DIGITAL MARKET (1996).
[31] The Indian Contract Act, § 10 (1872).
[32] The Indian Contract Act, § 2(h) (1872).
[33] *supra* note at 30.
[34] *Id.* at 10.

2. Smart Contracts & Enforceability

The Act does not say that the contract has to be a physical contract to be legal. The legality of an electronic contract can be lined under section 10A[35] of the Information Technology Act, 2000. Multiple pieces of literature have brought up this point that smart contracts are self-enforcing and do not require the assistance of parties. Now smart contracts are self-executory and not self-enforcing in nature. The computer codes cannot replace the legislation to enforce itself rather in case of breach the parties would always have the remedy to approach the court. Smart contracts keep track of the performance of parties but in case of any discrepancies in the contract or fault in coded agreement, the court would always analyse the computer codes. The power of enforceability does not shift to mere computer codes rather they still exist with the courts. Smart contracts merely guarantee the performance of contracts and not their enforceability. When the question of the enforceability of smart contracts occurs before the court of law they would not merely rely on the legal principles. The court along with the parties to the contract also has to acknowledge the economic aspect of the enforcement of smart contracts.

VI. Economic Analysis of Smart Contracts

By enforcement of smart contracts courts protect the interest of the parties who have mutually agreed to perform the obligations. Enforcement of contracts has dual benefits where it supports a healthy economy[36] and promotes global significance.[37] Multiple literatures have challenged the nature of smart contracts because they are immutable and susceptible to change. In case there are any changes in the circumstances, parties cannot modify it. This specific challenge to legality based on immutability is itself baseless.

1. Pareto Improvement

The main purpose of contracts is to enforce the agreement between two parties who have mutually agreed upon the terms and conditions. Hence, contracts are by default made for enforcement. Sometimes the contract shouldn't be enforced as it would not be economically

[35] The Information Technology Act, § 10A (2000).
[36]The World Bank, *Enforcing Contracts*, DOING BUSINESS (2019), https://subnational.doingbusiness.org/en/data/exploretopics/enforcing-contracts/why-matters.
[37]Shailak Jani, *Smart Contracts: Building Blocks for Digital Transformation*, RESEARCHGATE(Apr. 2020), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech

feasible[38] or would be against equity. But in general circumstances, contracts in everyday life should be enforced even if one party in future would not benefit significantly but does not face any loss. This voluntary nature of smart contracts draws the **Pareto improvement**[39]as even if one party is experiencing the benefit no party faces the loss. The implementation of a smart contract improves the condition of one party, but the other party does not suffer the loss and it also does not impact the non-parties of the contract. Now in case a party agrees to purchase something in return for the money as he believes the purchase would satisfy his needs. After the purchase is made the person feels that it was better without the action of spending money. But can he alter the purchase? No, as there was a contract which was implemented between the buyer and the seller and just because the buyer's expectations were not met does not permit him to alter the contract. Even if the contract is no significant improvement to one's life, it cannot be repudiated on their wish. This would hamper the social structure of society. The court would apply the Pareto Improvement principle to determine the impact of the enforcement of smart contracts on the parties to it. The immutability of smart contracts cannot be an obstacle to legality and enforceability.

2. *Efficient Reliance and Efficient Precaution*[40]

When two parties enter into the contract from an economic perspective, they need to analyse the risks involved in the transaction. Now there is a possibility that the promisee may not perform his obligation completely or perform only a part of it. One of the essential questions which can placed for smart contracts is why there is a need for assessment of such risk when the cost of transaction is comparatively lower than traditional contracts. Smart contracts although, do not rely on third-party costs and their execution is comparatively cheaper but such contracts follow a different ground of frustration. Smart contracts are programmed using codes which rely on technology and there are multiple chances of server hack, DoS attack, failed encryption along with similar grounds of frustration of traditional contracts. Hence, parties are reluctant to take such risk and calculate the inefficient cost.

[38]DANIEL H COLE & PETER Z GROSSMAN, PRINCIPLES OF LAW & ECONOMICS (Wolter Kluwer) (2011).
[39]ROBERT COOTER & THOMAS ULEN, LAW & ECONOMICS (Pearson) (2011).
[40]DANIEL H COLE & PETER Z GROSSMAN, PRINCIPLES OF LAW & ECONOMICS 244 (Pearson) (2004).

The total revenue which would be generated when the transaction gets included in the amount of loss in case there is a breach of contract by the parties. It would also include all the expenses which the promisor would incur when he enters into the contract. This is known as **efficient reliance**[41] When the parties enter into smart contracts, they also analyse the cost of non-performance. The efficiency in reliance would be achieved when the marginal cost (the increased cost) would be equal to the expected marginal benefit. Now the amount which would be spent by the promisor would be directly dependent upon the reliance on the gain from the performance by promise. Efficient reliance is a principle, which considers the final result of the contract and the revenue generated by it.

Now there can be a situation where the parties to the contract are aware of certain future contingencies and they decide to cover their losses by maximizing their profit. The promisor now calculates the amount in case of the breach along with compensatory charges. The extra expenditure which is incurred by the promisor has to be in coherence and should be incurred only if it reduces the cost of damages to some extent. This is known as **precaution efficiency** where the parties try to reduce the expected liability and incur some additional cost which could be **a marginal benefit**.[42] The cost which is incurred by the party to reduce their liability is their **marginal cost**. Examples of this can be hiring more workers or using more tools. These two principles stipulate that parties generally try to protect themselves before taking any undue risk. ambiguity.

VII. Conclusion and Suggestion

Implementation of CBDC is a step towards the future to welcome smart contracts. Although, there is a need for technological development, the understanding of smart contracts has to be altered. As the parties to the contract voluntarily enter into the agreement it is bound by the legal obligations stipulated under the contract law. Smart contracts are based on *consensus ad idem* and form a subset under e-contracts. The whole argument of smart contracts being a threat to traditional contracts cannot be accepted in reality. The self-enforcing nature of smart contracts does not make them a threat to contract law. Max Raskin demarcated between two types of contracts which depended upon time and effort to enforce the contract. One type can be

[41] *Id.* at 12.
[42] Pearson, *supra* note at 38.

classified as a strong contract and the other as a weak one. Strong contracts cannot be altered easily; neither by the courts nor the parties. On the other hand, weak contracts can be altered by the parties or modified by the courts in case of circumstantial change. Smart contracts fall under the ambit of strong contracts which cannot be modified. Hence, the legality of smart contracts cannot be questioned under the Act based on its nature of immutability. Alteration to contractual terms is a rare phenomenon and does not happen in everyday life.

Smart contracts are themselves not immutable, but acquire this feature when they are inserted into the blockchain technology.[43] Multiple debates regarding the immutability of smart contracts do not make them rigid rather the parties have full autonomy to decide what would be the conditions drafted in the codes. Such contracts are not isolated from the real world rather they have the support of oracles[44] that confirm any specific change of circumstances to the contract. The aspect of enforceability could be still decided by the courts in case parties decide to approach the court of law for legal interpretation.

The parties have the options of offer, counter offer and cross offer before converting the agreement into codes. Smart contracts are not enmasse which are based on similar circumstances and conditions. Contracts are right *in personem* which is unique to each party. Self-executory and language-specific are two features of smart contracts and when such contracts are placed on blockchain[45] it further gains its immutability character.

CBDC acts as a ray of hope for the acceptance of smart contracts and blockchain in India. The financial sector is one of the most crucial sectors contributing to the economy of the country. Although, the main highlight of the paper was CBDC and the use of smart contracts, it should not be limited to it. It is important to understand that smart contracts cannot be the panacea to all problems rather they can be a tool to solve such problems. Banks are the mitochondria of the economic structure of society. Smart contracts and blockchain can be implemented by the banks in the following areas:

[43] ŽELJKA MOTIKA, SMART CONTRACT AND TRADITIONAL CONTRACT IN THE LEGALTECH (2020).
[44] Ajar Rab, *Smart Contracts & Blockchain: The Panacea to the Unequal Bargaining Power of Consumers?* 8 IJCLP 40 (2020).
[45] Allie Grace Garnett, *How Smart Contracts Work with Blockchain: A Step-by-Step Guide*, BRITANNICA MONEY (May 18, 2023), https://www.britannica.com/money/decentralized-finance-defi (last visited Sept. 18, 2023).

- Insurance is one major area where banks can implement smart contracts and blockchain. The blockchain technology can be used to verify the documents and prevent any fraudulent transactions.[46] Further, it would also increase transparency as any changes can be viewed by all the parties to the insurance. It would reduce the intervention of third parties and also reduce the time spent on insurance claims. The process would be faster and at a lower cost. The blockchain used by the banks could maintain all the details relating to the parties and prevent delays in identification or risk analysis.
- Banks have faced problems due to bad mortgages where the parties could not perform their obligations.[47] Now in such cases mortgage contracts are executed there would be multiple formalities like interest rate, repayment date, other charges etc. If the party fails to perform its obligation the banks could initiate a legal suit against them and retain the property. This process could be lengthy and time-consuming. Smart contracts could play a huge role in mortgage contracts where in case of failure of performance, the contract would be executed in the same way as coded by the parties. The installments paid would be retained, and the property would be under the possession of the bank without even approaching the court.

[46] Pavlo Khropatyy, *How to Make a Smart Contract Work for the Insurance Industry*,INTELLIAS (Jan. 18, 2022), https://intellias.com/how-to-make-a-smart-contract-work-for-the-insurance-industry/
[47]Louwrens, *Why are smart contracts smart? MEDIUM (*July 10, 2023), https://louwjlabuschagne.medium.com/why-are-smart-contracts-smart-89aa168a8d0a.

NAVIGATING COPYRIGHT IN THE AI LANDSCAPE: OWNERSHIP AND FAIR USAGE

- ***Kusha & Sugandha Passi***[1]

Abstract

This research paper explores the intricate correlation between artificial intelligence (AI) and copyright legislation, particularly focusing on the legal challenges and implications surrounding AI-generated works. As artificial intelligence progresses, it progressively intrudes into domains typically associated with human creativity, prompting significant inquiries regarding authorship, possession, and equitable usage privileges. The paper critically examines key legal cases, precedents, and evolving regulatory frameworks, aiming to uncover the nuances of how copyright law is adapting to the digital age dominated by AI innovations. By exploring diverse jurisdictions such as the USA, EU, India, and China, the study highlights the lack of consensus on AI's role in creative processes and suggests potential legal reforms to address these emerging issues. This analysis is intended to contribute to the broader discourse among policymakers, legal scholars, and industry stakeholders, striving to forge a balanced approach that fosters innovation while protecting creators' rights in the AI landscape.

Keywords**:** *Artificial Intelligence, Intellectual Property, Copyright, Authorship, Ownership.*

[1] LL.M. (IPR), University Institute of Legal Studies (UILS) of Chandigarh University. Gmail: skusha2000@gmail.com& Assistant Professor, University Institute of Legal Studies (UILS) of Chandigarh University.

I. Introduction

In the swiftly evolving digital era, the convergence of artificial intelligence (AI) and copyright regulations unveils a multifaceted and fluid legal terrain. As AI technologies become increasingly sophisticated, they are not only capable of creating works that were once the exclusive domain of human creators, but are also challenging traditional notions of authorship, ownership, and fair usage. This research paper endeavours to delve into these intricate matters, scrutinizing the legal frameworks that oversee copyright concerning AI-generated creations, and the ramifications for creators, industries, and the public domain.

The emergence of AI has obscured the distinction between human creativity and machine-generated content, raising fundamental questions about who holds the copyright in works created with or by AI. Is it the programmer who develops the AI algorithm, the user who inputs data or parameters, or the AI itself? These questions are not merely academic; they have significant practical implications for the rights and remuneration of creators, the ability of industries to innovate, and the accessibility of cultural works to the public.

To navigate these complex waters, this paper will analyse key legal cases and precedents that have begun to shape the understanding of copyright in the AI era. For instance, the case of *Authors Guild v. Google Inc*[2]*. (2015)*, which dealt with the digitization of books by Google, sets a precedent for how courts view the digitization of copyrighted works and the concept of fair use. Similarly, the European Union's Copyright Directive (2019/790/EU) includes provisions specifically addressing the rights and responsibilities in the context of AI-generated content, offering a regulatory framework that could serve as a model for other jurisdictions.

The renowned statement by Justice Oliver Wendell Holmes Jr. encapsulates the crux of this discussion: *"The life of the law has not been logic; it has been experience."* This perspective holds particular significance in the realm of AI-generated creations, as the legal framework must adjust to the swiftly changing technological environment.

One of the most famous cases in this area is the *"Monkey Selfie"*[3] case, where a macaque monkey used a photographer's camera to take a selfie. The ensuing legal battle raised questions

[2] Authors Guild v. Google Inc 804 F.3d 202.
[3] Naruto v. Slater, 888 F.3d 418.

about who owned the copyright in the image: the photographer, the monkey, or no one at all. This case underscores the hurdles and intricacies of applying conventional copyright principles to works generated by AI.

Additionally, this paper will explore the concept of fair utilization in the domain of AI-produced content. Fair use regulations allow for the restricted application of copyrighted material without direct authorization from the copyright owner for activities including critique, analysis, journalistic reporting, instruction, academic pursuits, or investigation. Nevertheless, the application of these principles to AI-generated works introduces novel challenges, particularly in discerning the intent behind the creation and the transformative quality of AI outputs.

By examining these cases and concepts, this research paper aims to provide a comprehensive overview of the current state of copyright law in the AI landscape, identifying gaps and proposing potential solutions to ensure that the legal framework remains relevant and equitable in the face of technological advancements. Through this exploration, the researcher seeks to contribute to the ongoing dialogue among legal scholars, policymakers, and stakeholders about how to balance the promotion of innovation with the protection of creative rights in the age of AI.

1. Objective

The objective of this research paper is to explore the complex interplay between AI and copyright law, specifically examining the legal frameworks surrounding AI-generated works and their implications. The paper aims to address the blurring lines between human creativity and machine output, discussing authorship, ownership, and fair usage rights in the AI context. By analyzing key legal cases, precedents, and regulatory frameworks that are shaping copyright in the AI era, the researchers seek to propose solutions for a balanced legal landscape. Ultimately, this research contributes to the ongoing dialogue between legal scholars, policymakers, and stakeholders, ensuring the promotion of innovation while protecting creative rights in the age of AI.

2. Evolution Of Artificial Intelligence-Generated Content

The historical progression of AI-generated content has marked a notable area of growth over time. Initially, AI found its way into various domains like medicine, marketing, and education, aiding tasks such as screening submissions, data analysis, and improving learning experiences.[4] As AI technologies matured, they began to actively impact organizational processes, introducing novel approaches to organizational management.[5]

The incorporation of AI into architectural design, for instance, brought about a revolutionary shift in the construction industry, showcasing AI's transformative potential in creative fields.[6] However, the utilization of AI for content creation has also sparked ethical concerns, particularly regarding issues like plagiarism and copyright violations. Educators have been called upon to enhance their understanding of AI to ensure its responsible and ethical application, especially in areas like medical education.[7]

Furthermore, the misuse of AI-generated text has been flagged as a potential tool for spreading misinformation in the media, underscoring the importance of vigilance and awareness surrounding AI technologies.[8] The evolution of AI-generated content has also left its mark on sectors such as tourism and hospitality, where novel AI models have introduced innovative methods for crafting marketing content.[9]

Moreover, the rapid progress in natural language processing and neural network technologies has accelerated AI's evolution in shaping educational landscapes, indicating a shift towards automated decision-making and multimedia generation tools.[10]

Thus, the historical journey of AI-generated content has witnessed significant advancements across diverse sectors, from streamlining organizational processes to transforming creative

[4] Flanagin, Annette, et al., Nonhuman "authors" and implications for the integrity of scientific publication and medical knowledge, 329 Jama, 637 (2023).
[5] Murray, Alex, et al., Humans and technology: forms of conjoined agency in organizations, 46 AMR, 552-571 (2021).
[6] Hegazy, Muhammad, et al., Evolution of ai role in architectural design: between parametric exploration and machine hallucination, 2 MSA Engineering Journal, 262-288 (2023).
[7] Boscardin, Christy K., et al., Chatgpt and generative artificial intelligence for medical education: potential impact and opportunity, 99 Academic Medicine, 22-27 (2023).
[8] Kreps, Sarah E., et al., All the news that's fit to fabricate: ai-generated text as a tool of media misinformation, 9 JEPS, 104-117 (2020).
[9] Tuomi, Aarni, et al., Ai-generated content, creative freelance work and hospitality and tourism marketing, ICTT 2023, 323-328 (2023).
[10] Smith, Anna, et al., Guest editorial: artificial intelligence and composing just education futures, 23 ETPC, 1-5 (2024).

industries, while also prompting crucial ethical considerations. As AI continues to progress, it becomes imperative for stakeholders to navigate its evolving landscape responsibly, ensuring the ethical and effective utilization of AI-generated content.

II. COPYRIGHT FUNDAMENTS

1. Defining Copyright

a. *Understanding the Concept:*

Copyright is a legal principle granting creators of original works exclusive rights over their creations, including literary, artistic, musical, or cinematic works.Its objective is to uphold equilibrium by safeguarding the interests of creators while also facilitating public access to information and artistic expression.

b. *Core Principles:*

Copyright law grants temporary monopolies to creators, incentivizing them to produce new works, as they can profit from their creations. In exchange, these works eventually enter the public domain, allowing others to use them freely.

2. Exclusive Rights Granted by Copyright

a. *Reproduction Right:*

Creators can control who can make copies of their work, preventing unauthorized duplication.

b. *Distribution Right:*

Creators retain the right to determine the distribution of their work, encompassing sales, rentals, or digital downloads.

c. *Derivative Works Right:*

Creators can decide if others can create new works based on their original, such as sequels, adaptations, or translations.

d. *Public Performance Right:*

Creators can control public performances of their work, including live shows, broadcasts, and streaming.

e. *Display Right:*

Creators possess the authority to regulate the public display of their visual works, whether exhibited in galleries, online platforms, or other settings.

3. Originality in Copyright Protection

a. *Importance of Originality:*
   To qualify for copyright protection, a work must exhibit a certain degree of creativity and not merely replicate an existing work.
b. *Threshold of Originality:*
   Each jurisdiction has its own standard, but generally, a work must show a minimal degree of creativity and individuality to qualify for copyright.
c. *Copyright vs. Ideas:*
   Copyright legislation protects the specific articulation of concepts, rather than the concepts themselves.

III. OWNERSHIP OF AI-GENERATED WORKS

Deciphering the ownership of AI-generated content presents a nuanced issue involving legal, psychological, and ethical dimensions. Traditional copyright frameworks face challenges when applied to AI-generated works.[11] This blurring of lines between authorship and ownership prompts discussions on whether AI should be acknowledged as the rightful owner of its creations.[12] Users interacting with AI-generated content may not adhere to conventional ownership norms but may still perceive themselves as authors, highlighting the importance of understanding both objective and subjective aspects of control in human-AI interactions.

Psychological perspectives on ownership emphasize its dual nature, encompassing both attitudes and tangible objects.[13] These psychological underpinnings significantly shape how individuals perceive and engage with AI-generated content. Moreover, ethical considerations surrounding AI, particularly in sectors like healthcare, raise concerns regarding privately owned AI solutions

[11]Matulionytė, Rita, et al., Copyright in ai-generated works: lessons from recent developments in patent law, 19 SCRIPT-ed, 5-35 (2022).
[12] Adaka, Eloghene E., et al., Lessons for nigeria: determining authorship and inventorship of artificial intelligence generated works, 2 JIPIT, 15-48 (2022).
[13] Pierce, Jon L., et al., The state of psychological ownership: integrating and extending a century of research, 7 RGP, 84-107 (2003).

trained on public data.[14] Upholding transparency and legal compliance in AI systems generating content is crucial for mitigating adverse effects and safeguarding intellectual property rights.[15]

Legally, determining authorship and inventorship of AI-generated works challenges existing intellectual property rights frameworks. The intersection of AI and moral rights further complicates the landscape of ownership and control over AI-generated content.[16] Effective regulation of AI requires transparency and accountability to prevent infringements and ensure responsible AI deployment. Proposals advocating for a collective approach to AI data governance suggest universal data ownership rights to uphold trustworthiness in AI applications.[17]

1. Legal Frameworks and Approaches

a. India:

In India, the Copyright Act, 1957, is the primary legislation governing copyright. As of now, there is no specific provision addressing AI-generated works. The Act attributes authorship to natural persons, indicating that AI systems are not considered authors. However, the debate is ongoing, and future legal interpretations or updates may address AI-generated works.

b. *United States:*

U.S. copyright law, as per the Copyright Act of 1976, also attributes authorship to human creators. The U.S. Copyright Office has explicitly stated that it will not register works produced by machines or nature without human intervention or authorship. This means that in the U.S., ownership of AI-generated works remains unclear, and the responsibility typically falls on the human who programmed or facilitated the AI's creation.

c. European Union:

In the EU, the Copyright Directive 2019/790 mentions the "use of artificial intelligence and other automated systems" but does not explicitly address ownership. The Directive focuses on the liability of online content-sharing platforms. As with other jurisdictions,

[14] Morley, Jessica, et al., The ethics of ai in health care: a mapping review, 260 SSM, 113172 (2020).
[15]Wörsdörfer, Manuel, et al., Mitigating the adverse effects of ai with the european union's artificial intelligence act: hype or hope, 43 GBOE, 106-126 (2023).
[16] Miernicki, Martin, et al., Artificial intelligence and moral rights, 36 AI Soc, 319-329 (2020).
[17] Lewis, David, et al., A rights-based approach to trustworthy ai in social media, 6 SM + S, 205630512095467 (2020).

the lack of explicit rules suggests that AI-generated works are not considered authored by the AI itself, and ownership may be attributed to the human operator or developer.

d. China:

Chinese copyright law follows a similar principle, attributing copyright to the "creator" of a work, which traditionally refers to a human being. However, China's rapid advancements in AI have sparked discussions on updating the law to address AI-generated works. Currently, there is no clear legal framework, and ownership is likely to rest with the human operator or developer.

2. Can AI be considered an Author?

The debate on considering AI as an author revolves around the concept of creativity and originality. While AI can produce outputs that mimic human creativity, it lacks the consciousness and intent associated with traditional authorship. Some argue that AI-generated works should be considered "joint works" between the AI and its human programmer, while others suggest a new legal framework is needed.

3. Comparing Approaches:

India and the EU: Both countries rely on existing laws that attribute authorship to human creators, leaving AI-generated works in a legal gray area.

United States: The U.S. has a clear stance against AI as an author, requiring human intervention for copyright registration.

China: Like India and the EU, China's current laws do not directly address AI-generated works, but the country is more likely to adapt its laws to address the evolving technology.

IV. POTENTIAL SOLUTIONS FOR OWNERSHIP OF AI-GENERATED WORKS

1. Attribution to Human Programmers

One potential solution is to attribute copyright to the human programmer or developer who created and programmed the AI system. This approach acknowledges that the AI is a tool devised and managed by a human, thus placing responsibility for the output on the human creator. However, this solution may diminish the creative input of the AI, and determining

the programmer's exact contribution to the final output, particularly in intricate AI systems, could pose challenges.

2. Joint Authorship between AI and Human

Another approach is to consider both the AI and its human operator or programmer as joint authors, thus sharing copyright ownership. This recognizes the AI's role in the creative process alongside the human's guidance and training of the AI. In such a scenario, rights and responsibilities such as licensing, distribution, and adaptation of the work would need to be negotiated and agreed upon by both parties. Establishing joint authorship could, however, introduce legal complexities, especially in cases involving multiple humans in the AI's development or operation, and could raise questions about the AI's legal status and accountability.

3. Sui Generis Rights for AI-Generated Works

Alternatively, a sui generis approach could entail creating a distinct category of rights tailored specifically for AI-generated works. This approach acknowledges the unique nature of AI-generated content, which stems from a combination of human input and machine processing. Under this model, rights might be assigned to the entity responsible for operating the AI, such as the company or organization utilizing the system. Specific regulations would govern the use, licensing, and distribution of AI-generated works. However, implementing a sui generis system would necessitate substantial legal and policy development, as well as international coordination to ensure consistency across jurisdictions. It could also spark debates regarding the optimal balance between incentivizing innovation and safeguarding public access to AI-generated content.

V. FAIR USE AND AI

In the era dominated by AI, the intersection of copyright law and fair use has become a topic of intense debate. Fair use, a legal principle outlined in the Copyright Act of 1976, permits the utilization of copyrighted materials under specific circumstances.[18] However, the emergence of AI technologies has raised inquiries about how copyright law should apply to content generated

[18] Pressman, Rebecca, et al., Fair use: law, ethics and librarians, 47 JLA, 89-110 (2008).

by AI systems. Scholars have engaged in discussions regarding whether AI-generated outputs should be eligible for copyright protection, emphasizing the necessity for clear guidelines in this evolving field.[19]

The intricate nature of fair use within copyright law is further underscored by the Supreme Court, which regards fair use as a means of safeguarding the First Amendment, preventing undue restrictions on cultural activities imposed by copyright laws. This underscores the pivotal role of fair use in reconciling the rights of copyright holders with society's requirement for access to information and cultural creations.

With the continuous advancement of AI, ensuring fairness within AI systems has emerged as a pressing concern. Developers are urged to prioritize social and ethical considerations in designing AI models and to actively address biases inherent in these systems. However, the focus on fairness in AI often centers on algorithmic and mathematical aspects, sometimes neglecting broader ethical implications.

Additionally, the demand for fairness certification in AI systems has prompted the creation of frameworks like the Fairness Score and standardized processes to detect biases, ensure fairness, and establish consistent procedures for evaluating AI fairness.[20] This standardization is critical as AI systems become increasingly prevalent across various domains, highlighting the importance of transparency and accountability in AI development and deployment.

In the domain of AI ethics, principles such as fairness, accountability, and transparency form the foundation of socially responsible AI algorithms.[21] Trustworthy AI frameworks emphasize the establishment of trust throughout the development, deployment, and utilization of AI systems to unlock their full potential while considering their societal impact.[22]

As discussions surrounding fair use and copyright in the AI era progress, it is essential to consider the nuances of fairness metrics in machine learning, the challenges posed by bias in AI

[19] Asay, Clark D., et al., Independent creation in a world of ai, 14 FIU Law Review, (2020).
[20] Avinash, Agarwal, et al., Fairness score and process standardization: framework for fairness certification in artificial intelligence systems, 3 AI and Ethics, 267-279 (2022).
[21] Cheng, Lu, et al., Socially responsible ai algorithms: issues, purposes, and challenges, 71 JAIR, 1137-1181 (2021).
[22]Thiebes, Scott, et al., Trustworthy artificial intelligence, 31 Electronic Markets, 447-464 (2020).

algorithms, and the significance of open science practices in addressing these issues.[23] Collaborative efforts across disciplines and industries are indispensable for promoting fairness in AI and navigating the intricate ethical and legal landscape surrounding AI technologies.

1. Fair Use and Its Transformative Nature

Fair use serves as a legal doctrine within copyright law, permitting the utilization of copyrighted material without the owner's authorization for particular aims, such as critique, commentary, journalistic reporting, instruction, academic pursuits, or investigation. It operates as a flexible doctrine subject to interpretation by courts on a case-by-case basis.

A fundamental element of fair use involves the transformation of the original work into something novel, contributing value or a fresh interpretation to the original content. When a use is transformative, it diminishes the likelihood of being deemed an infringement, as it does not directly impinge on the market value of the original work.

2. The Challenges in Applying Fair Use to AI

a. *Difficulty in Determining the Purpose and Character of AI Use:*
   AI systems frequently train on extensive datasets that include copyrighted material, posing challenges in evaluating the purpose and nature of the use. Is the AI using the material for research, training, or to create a derivative work? The motivations behind AI's use of copyrighted content may not always align with the traditional human-driven fair use scenarios.
   Moreover, the lack of human intent or conscious decision-making in AI's use of copyrighted material can complicate the analysis. Fair use typically considers the user's good faith and the purpose of the use, which are less clear in AI-driven processes.
b. *Concerns regarding the quantity and significance of copyrighted material utilized:* One of the fair use factors is the amount and substantiality of the copyrighted work used. In AI contexts, the sheer volume of data consumed can be immense, potentially raising concerns about excessive use.

[23]Castelnovo, Alessandro, et al., A clarification of the nuances in the fairness metrics landscape, 12 Scientific Reports, (2022).

AI models frequently necessitate extensive datasets for effective training. However, discerning what constitutes a 'substantial' portion becomes challenging when dealing with intricate algorithms that may or may not retain recognizable elements from the original work.

c. *Infringement Risk without Human Intervention:*

AI-generated outputs may inadvertently incorporate copyrighted material, especially when the AI is trained on a diverse range of content. Lack of human oversight can lead to unintentional infringement, creating a challenge for determining liability.

d. *Balancing Rights and Innovation:*

Applying fair use to AI prompts questions about striking a balance between safeguarding creators' rights and fostering technological innovation. Integrating copyrighted material into AI development is essential for advancing AI capabilities, but it also carries the risk of undermining the rights of the original creators.

e. *Analyzing potential fair use scenarios in the context of AI*

Analyzing potential fair use scenarios in the context of AI involves navigating a complex interplay between copyright law and transformative uses of copyrighted material. One significant area of concern is the training of AI models on copyrighted data. When AI algorithms are trained using copyrighted material, several considerations come into play. For instance, if AI is employed for educational or research purposes, such as analyzing historical documents or scholarly texts, it may be argued that such use falls under fair use. This argument rests on the transformative nature of the AI's analysis, which aims to enhance understanding rather than simply replicate the original material. Similarly, using a limited subset of copyrighted data for the development and testing of AI algorithms might be considered fair use, provided it does not significantly affect the market value of the original works. Moreover, the use of public domain or openly licensed data in AI training is typically viewed as fair use since the original creators have already consented to the reuse of their work. Additionally, if an AI's training process results in a new product or service that is substantially different from the original works, it could be argued that the use is transformative and therefore fair.

Moving beyond training, the creation of derivative works by AI based on copyrighted materials raises further fair use considerations. For example, if an AI-generated work serves as a parody or

satire, it may qualify as fair use as it comments or critiques the original while adding new meaning or social commentary. Similarly, AI-generated works that provide critical analysis or reporting on original content could be deemed fair use if they aid in understanding the material.

Moreover, transformative art generated by AI, which combines elements from various copyrighted sources to produce original pieces, might be considered fair use if the resulting work possesses a distinct artistic identity. Similarly, AI-generated derivative works used for comment or review purposes, such as illustrating a critique, could potentially be classified as fair use.

Nevertheless, it's important to recognize that fair use is a nuanced legal concept, and its implementation depends on the particular circumstances of individual cases. As AI technology progresses, it will be vital to continuously refine fair use principles to accommodate emerging creative and analytical potentials while upholding copyright law. Ultimately, the assessment of whether a specific use is fair will rely on the particular context and the interpretation of courts.

Navigating the complexities of copyright in the AI landscape presents several challenges for creators, developers, and legal professionals. As AI technologies, especially those related to machine learning and content generation, become more advanced, these challenges and the need for clear guidelines and reforms become more pronounced.

VI. PRACTICAL CONSIDERATIONS AND RECOMMENDATIONS

1. *Challenges for Creators and Developers*

a. *Attribution and Authorship:*

Determining the authorship of content generated by AI is complicated. Traditional copyright laws are designed to protect human creators, but AI-generated content often blurs these lines, raising questions about originality and ownership.

b. *Infringement Risks:*

AI can process and generate content by learning from vast datasets, some of which may include copyrighted material. This raises risks of unintentional copyright infringement, as the AI may create content that is too similar to existing copyrighted works.

c. *Fair Use Uncertainty:*

The application of the fair use doctrine is unclear in the context of AI. Developers and creators often struggle to understand whether using copyrighted material to train or operate AI systems falls under fair use, due to the transformative nature of AI processes.

d. *Global Legal Disparities:*

Copyright laws vary significantly across countries, making it difficult for AI developers and content creators to navigate these regulations effectively, especially in a globally connected digital environment.

e. *Digital Rights Management (DRM):*

The use of DRM to protect copyrighted works can conflict with the operation of AI systems, especially when they need to analyze and learn from protected content.

f. *Licensing Complexity:*

The licensing of copyrighted materials for use in AI training sets is not straightforward, as standard licensing agreements may not cover the use of data in AI applications.

2. Implementing Best Practices

Protecting Copyrighted Works from Unauthorized AI Use

a. *Clear Licensing Agreements:*

Ensure that all copyrighted material has clear licensing terms that specify the scope of allowed use, including whether the material can be used to train AI models.

b. *Use of Watermarking and DRM:*

Implement digital watermarking and DRM solutions to monitor and control the distribution and use of copyrighted materials, making it harder for these works to be used without authorization.

c. *Active Monitoring:*

Use technology to actively monitor and detect unauthorized use of copyrighted works, especially in digital platforms where AI-generated content is frequently shared.

d. *Collaborative Approaches:*

Engage in partnerships with AI developers to create shared frameworks and standards for respecting copyright in AI-generated content.

e. *Transparency in AI Training:*

Disclose the sources of training data and seek permissions where necessary, fostering transparency and ethical practices in AI development.

Using AI Tools in a Way that Respects Copyright

a. *Seek Explicit Permissions:*
   Before using copyrighted materials to train or improve AI models, obtain explicit permissions from copyright holders, possibly through licensing agreements.
b. *Utilize Open Licenses:*
   Where possible, use content covered by open licenses (e.g., Creative Commons) that allow for broader uses, including training AI systems.
c. *Fair Use Analysis:*
   When employing copyrighted material, it is crucial to undertake a thorough fair use assessment, considering factors such as the purpose, nature, extent, and impact of the use on the potential market or value of the copyrighted work.
d. *Documentation and Due Diligence:*
   Maintain detailed records of how materials are used in AI processes, including training datasets, to demonstrate due diligence and respect for copyright laws.
e. *Ethical AI Development:*
   Adopt ethical guidelines for AI development that include respect for intellectual property rights alongside other considerations like privacy and transparency.

Potential Legal Reforms

a. *Clarify Copyright Rules for AI:*
   Legislatures could develop specific guidelines or laws that clarify how copyright applies to AI-generated content and the use of copyrighted materials in AI training.
b. *Create a Safe Harbor for AI Research:*
   Implement safe harbor provisions that protect AI researchers and developers from infringement claims when copyrighted material is used in non-commercial research and development under certain conditions.
c. *Establish AI-Specific Licensing Models:*

Develop new licensing models that are tailored for AI use cases, including expanded rights for training materials and clear terms for the use of AI-generated content.

d. *Digital Single Market Initiatives:*
   For countries in regions like the European Union, harmonize copyright laws to create a more consistent legal framework across borders, particularly for digital and AI-generated content
e. *Update Fair Use Guidelines:*
   Provide clearer, more detailed guidelines on how the fair use doctrine applies to the use of copyrighted materials in AI contexts, possibly including examples or illustrative scenarios.

By addressing these challenges and adopting these best practices, creators and developers can navigate the evolving landscape of copyright and AI more effectively, fostering innovation while respecting the rights of copyright holders. Legal reforms that keep pace with technological advancements will be crucial in supporting these efforts and ensuring a balanced approach to copyright in the digital age.

VII. Conclusion

This research paper has explored these issues through a comprehensive analysis of legal frameworks, notable case studies, and a comparison of approaches across different jurisdictions. By examining the current state of copyright law in the context of AI, the researcher has identified gaps and proposed potential solutions to ensure a balanced and equitable legal framework that promotes innovation while protecting creative rights.

The discussion on the ownership of AI-generated works has revealed a legal gray area, with existing laws often attributing authorship to human creators. The researcher has proposed three potential solutions: attribution to human programmers, joint authorship between AI and humans, and the creation of sui generis rights specifically for AI-generated content. Each solution presents its own set of challenges and complexities, underscoring the need for careful consideration and ongoing dialogue among legal scholars and policymakers.

Furthermore, the researcher has delved into the concept of fair use in the AI era, highlighting the challenges of applying traditional copyright principles to AI-driven processes. The

transformative nature of AI outputs and the lack of human intent or decision-making in these processes complicate the analysis of fair usage. This research has emphasized the importance of clear guidelines and the need for a nuanced understanding of fairness metrics and ethical implications in machine learning.

Finally, this paper has offered practical considerations and recommendations for creators, developers, and legal professionals navigating the complexities of copyright in the AI landscape. These include best practices for protecting copyrighted works, such as clear licensing agreements, digital watermarking, and active monitoring, as well as suggestions for using AI tools in a way that respects copyright, such as seeking explicit permissions and utilizing open licenses.

In summary, as AI continues to evolve and shape various industries, including creative fields, it is imperative to adapt legal frameworks to address the unique challenges posed by AI-generated content. The researcher hopes that this study contributes to ongoing discussions and informs future policy developments, ensuring a harmonious relationship between technological advancements and the protection of creative rights in the age of AI.

DIGITAL LENDING: BNPL CASE AND RBI'S REGULATORY CONUNDRUM

- ***Yash Vardhan Singh***[1]

Abstract

This article makes an effort to discusses the emerging and fast paced growth of Fintech in India specifically the Buy Now Pay Later system and the RBI's Guidelines on Digital Lending, released in September 2022. It discusses the interplay of these guidelines while discussing the needs of such guidelines along with the obstruction its causing to the growing Indian Fintech ecosystem especially the Digital Lending. The article provides a brief summary of BNPL and its importance and growth story along with the insight into the Guidelines released by RBI to contain this growing sector. The article also aims to shed light on the implications for different business models and entities, including payment aggregators, buy-now-pay-later platforms, and first-loss default guarantee arrangements, by discussing compliance and disclosure requirements for regulated entities, digital lending apps, and lending service providers.

Keywords*: Digital Lending, Buy Now Pay Later, RBI's Digital Lending Guidelines, 2022, Consumer Protection, Data Privacy.*

[1] National University of Study and Research in Law, Ranchi. Gmail: singh.yashvardhan97@gmail.com

Introduction

The way businesses and consumers borrow money has significantly changed as a result of digital lending through websites and apps. Fintech-led digital lending blends traditional banking services with cutting-edge technology. As a result, borrowing has become easier, loans are disbursed more quickly and with very less paperwork, and a wider range of people can now access credit. During the Covid-19 pandemic, digital lending increased by tenfold.

In the post Covid years, the buy now pay later industry has been one of the fastest-growing industries in India and what is absolutely mind-blowing is that the BNPL market is growing so fast in India, that it achieved an insane growth rate of 569% in 2020 and 637% in 2021. But on 20th of June 2022, the Reserve bank of India made an announcement that shook the entire BNPL industry. This notification disallowed non-bank prepaid wallets and prepaid cards from loading credit lines into these platforms.

In simple words, this is a huge blow to some of the fastest-growing Indian start-ups like Slice, Uniorbit, and Jupiter and until now these start-ups with their credit lines have played a vital role in taking financial inclusion and digitalization to the next level in India.

So, the question is, what is the problem with the buy now pay later industry? Why is the RBI hindering its growth with these regulations in spite of the industry growing at such a rapid pace?

The research article will try to give prospective on the BNPL and its regulatory conundrum while diving deep into RBI's Digital Lending Guidelines, 2022.

Buy Now, Pay Later or BNPL – The new age Digital Lending

You may have noticed the option to pay later if you have lately made any online purchases. Although Buy Now, Pay Later options are increasingly common on e-commerce websites and apps, you may also see them at big malls or even at some retail establishments. Typically, in order to get that new, pricey item, you would need to save money each month. However, nobody wants to do that, especially if the item is currently on some kind of sale but might not be in next few days. This is where Buy Now, Pay Later (BNPL) handiness comes in. BNPL firms are capitalizing on the appeal of making payments later in a manner similar to how Credit Cards captured markets.

In the past, a credit card or line of credit was the answer to this issue. However, it goes without saying that obtaining a credit card in India isn't always simple, and that once you do, you'll have to pay interest and many other fees. This is where "Buy Now, Pay Later" (BNPL) shows up. BNPL startups are capitalizing on the appeal of deferring payments in a similar manner to how you would use a credit card by making the process clear-cut, simple, and easy.

BNPL v Credit Cards – the Difference

Both credit cards and BNPL are deferred repayment options for borrowers, although there are a few key differences between the two credit products.

1. ***Eligibility***

In case of credit cards, the eligibility is decided based on the customers' annual income along with their credit score. On the other hand, BNPLs are small-ticket loans with no such eligibility criteria and can be obtained very quickly.

2. ***Onboarding Fees***

Many credit cards come with added costs of borrowing like joining fees and annual fees while the BNPL platforms do not charge any fee for joining.

3. ***Interest***

Usually, credit cards offer around 45 days of interest-free credit period while in the case of most of the BNPLs the interest-free credit period goes up to around 15 days.

4. ***Acceptance***

Credit cards are accepted almost universally, while acceptance of BNPL is as of today limited to a few partnering merchants. Although, the number of BNPL partners is increasing at a breakneck pace.

5. ***Credit Limit***

The credit limit on credit cards varies greatly depending on customer's credit history. However, for BNPL, credit limit ranges between Rs 2,000 to Rs 1, 00,000.

As a result of this complexity only 3% of Indian Population has a Credit card while a whopping 97% of Indian do not own any sort of Credit Card. This is where BNPL comes in.

The primary distinction between BNPL and credit cards, despite their apparent similarities, is how they are implemented. There are only 30 million credit card users in India due to the country's challenging credit card application process. Credit card issuers have set high standards, but BNPL startups like Slice, Zest Money, Simple, Lazy Pay, and Uni are lowering the bar. Almost anyone can purchase now and pay for it later; all you have to do is supply information such as your PAN and Aadhaar number.

These BNPL providers use their own algorithms, not credit scores, to decide how much credit to give you based on your transaction history and location and once you've been a BNPL customer for some time and as long as you've been in good standing and you've paid your off your loans, they'll increase your credit limit, too.

BNPL – Business Model of Profit

For BNPL startups, there are a few different revenue streams. First, merchants provide it. BNPL businesses charge merchants anything from 2 to 8% of the purchase price, just like credit card companies and point-of-sale suppliers do. For instance, if you buy shoes for Rs 3000, the BNPL companies pay the show seller just Rs 2900 maybe and charge the customer Rs 3000 and keep Rs 100 as their gain. Because of the advantages of working with the BNPL supplier, the merchant is now happy with this. First of all, because customers who previously might not have been able to purchase expensive things in their marketplace or store can now, they witness an increase in conversions and average transaction values.

In summary, partnering with a BNPL company essentially brings businesses additional high-paying consumers. The best part is that merchants don't actually shoulder any of the risk here the BNPL company pays them right away on behalf of the customer so those monthly EMIs that the customer is paying do not go to the merchant the merchant has already been paid in full instead the end customer pays the EMIs to the BNPL company who is taking all of the risk in their hands. Hence, it's a win-win situation for merchants, the BNPL as well as the borrowers.

The other source of revenue comes from late fees, akin to the Credit Card companies. According to BankBazaar, these fees can be a percentage ranging anywhere from 2 to 8 per cent of the principal loan amount, or they can be a flat fee.

BNPL – Problems and need of Regulation

According to research published by RBI in November 2021, over 30% of digital lending apps asked for user's location and camera access while 21% of apps asked for contact access in the phone. The investigation further discovered that over 600 of the 1100 lending apps available for android users were unauthorized and illegal and carried the danger of user accounts being stolen, phishing attempts, and identity theft among other cyber-crimes.

Many Indian BNPL clients are unaware of the existence of credit scores and are unaware that delaying paying off their debt might permanently harm their financial reputation. It is very easy to apply for BNPL from four or five different platforms and borrow up to one lakh rupees with a minimal amount of paperwork and no evidence of income at all. This places those with lower economic intelligence in a "debt trap" from which it can occasionally be challenging to escape.

There have also been reports of BNPL enterprises failing to submit defaults to credit bureaus, growing too quickly to scale their due diligence, and engaging in improper KYC or credit bureau checks.

The Digital Lending sector has been organized for a long time since its inception. The entire Digital Lending ecosystem has operated in an unregulated manner since ages and need for regulating this sector had been alarming.

RBI Guidelines and Conundrum

The RBI has formulated the Digital Lending Guidelines ("DLG") 2022[2] which would regulate all these instant credit and digital lending platform. The Guideline seeks to:

- Ensure Consumer protection through strict compliance
- Formulate technology and data requirement to be followed by Regulated Entities (REs) and Digital Lending Applications (DLAs)

[2] Guidelines on Digital lending by RBI notification no: RBI/2022-23/111 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12382&Mode=0 (Accessed 16 November 2023)

- Regulate digital lending ecosystem in the country where RE engage in commercial relationship with Lending Service Provider (LSPs) and DLAs

Let us dwell deeper into these Guidelines –

1. To whom the Guidelines would be Applicable

The Guidelines are applicable to "Regulated Entities" or "REs" which includes digital lending services "DLS" extended by

- All Commercial Banks
- All Co-operative Banks
- NBFCs including housing finance companies

The scope of Guidelines to the digital lending will include lending operations such as credit evaluation, loan approval and payout, recovery, as well as associated customer support that require a physical interface with the borrowers.

The Guidelines also provided a definition for "Digital Lending Apps"[3], as a web- and mobile-based applications with a user interface that support digital lending services. An example of this would be a bank's mobile banking app, which allows a user to apply for a loan directly from their phone. A DLA may be run directly by a RE or through an LSP.

Lending Service Providers[4], also known as LSPs, are referred to as middlemen between the borrower and the RE. These are organizations that function as the RE's agent and handle one or more of the RE's duties, such as monitoring, recovery of particular loans, underwriting support, and pricing support.

The Guidelines made it clear that a RE's outsourcing of any activity to a DLA or an LSP does not relieve the RE of its responsibility to follow the current RBI outsourcing guidelines. Furthermore, it is imperative for REs to guarantee that LSPs and DLAs adhere to the Guidelines.

2. Emphasis on the Protection of Customer

[3] Digital Lending Guideline, 2022,clause 2.4
[4] Digital Lending Guideline, 2022, clause 2.5

According to the Guidelines, no third-party account, including an LSP or a DLA account, may be used for loan disbursement or repayment. Credit disbursements and repayments must happen directly between the borrower's bank account and the RE except under some circumstances.

- Loan disbursals for specific end-uses;

- Statutory or regulatory mandates; and

- Co-lending transactions, which are agreements involving the joint contribution of a credit facility along with risk and reward sharing.

The Buy Now Pay Later ("BNPL") models are made possible by the exemption for particular end uses, which enable REs, LSPs, and DLAs to disburse the loan amount directly to the merchant.

In addition to this, each RE needs to make sure that their LSPs have a Nodal Grievance Officer in place to handle any complaints regarding fintech, digital lending, and DLAs. Furthermore, the credit borrower may file a complaint on the Complaint Management System Portal under the RBI Integrated Ombudsman Scheme, or "RB-IOS," if the borrower files a complaint against a RE or if the LSP the RE engages does not resolve the complaint within 30 days.

3. Transparency and Disclosures

The RE is required by the Guidelines to submit a **Key Fact Statement**, or KFS, in a standard format. A Key Fact Statement ("KFS") must be created by REs and given to the borrower prior to the loan contract being executed. All relevant information, such as the recovery mechanism, the grievance redressal officer's details, the cooling-off period, and the Annual Percentage Rate ("APR"), which is the Effective Annualized Rate that is charged to the borrower, must be in the KFS.

REs are required to give borrowers a **"Cooling-off Period",** or window of opportunity, during which they can return the digital loan plus the appropriate APR without incurring penalties. The cooling off period must be at least three days for digital loans with tenures of seven days or longer, and it cannot be less than one day for digital loans with tenures of less than seven days. It is still appropriate to allow the pre-payment option after this time.

In order to avoid charging the borrower, REs must make sure that the fees, charges, etc. paid to the LSPs are paid by them. In addition, penalties and charges will be assessed based on the balance of the outstanding loan. In addition to this, annual penalty charge rate must be included in the KFS. This is due to fact that some of the hidden fees associated with the loans that were provided had exorbitant processing fees totaling 35–40% of the loans.

It is mandatory for REs to make sure that any fees that are owed to the LSPs are paid by the RE to the LSP directly, rather than the LSP charging the borrower. Furthermore, the rate of any penal interest or charges that the RE imposes on the borrowers must be declared up front in the KFS and must be applied to the remaining balance of the loan.

In order to determine an LSP's technical capability, data privacy policy, fairness in conduct, and ability to adhere to applicable laws and regulations, REs must perform extensive due diligence prior to working with them. Moreover, the REs must routinely assess the LSPs' operations. Finally, in order to guarantee that the LSPs are operating responsibly and adhering to the Circular on "Outsourcing of Financial Services - Responsibilities of regulated entities employing regulatory agents," REs must advise the LSPs on loan recovery.[5]

4. Data Collection and Privacy Policy

According to the Working Group's report[6] (issued on November 18, 2021ma), there have been numerous complaints alleging that the DLAs have been collecting high-risk data and using it to harass borrowers as well as the people in their Contacts. The RBI has ordered that data collection by REs, LSPs, and DLAs be need-based and require explicit consent prior to data. Access to contact, file, media, and other mobile phone data is prohibited. One-time consent to use the microphone, camera, location, etc. can be obtained for KYC purposes. The borrower must be informed of the reasons behind the request for consent before it can be granted.

[5]Outsourcing of Financial Services - Responsibilities of regulated entities employing Recovery Agents , RBI Notification number : RBI/2022-23/108 https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT1085404663A577943BBB344A37057621C17.PDF(Accessed 19 November 2023)

[6]Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps, RBI (November 18, 2021) https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DIGITALLENDINGF6A90CA76A9B4B3E84AA0EBD24B307F1.PDF(Accessed at 22 November 2023)

RE must ensure that every LSP and DLA they work with has a very thorough privacy policy that outlines any third parties that may be permitted to obtain personal information through the LSPs or DLAs, as well as the kinds of data that may be stored and for how long and limitation on use of such data.

LSPs and DLAs only need to keep the bare minimum of data in order to function. REs are in charge of maintaining the security and privacy of the customer's personal data. A detailed and unambiguous data policy that specifies what data can be stored, how it can be used, how it will be destroyed, and other details needs to be implemented and posted on the RE's website and app store. In addition to the data policy, there must be a thorough privacy policy in place that makes public the identity of any third party authorized to collect data. The information has to be kept on servers located in India that abide by all applicable rules and laws. Finally, REs need to ensure that biometric data cannot be collected unless authorized by statute.

Primary reasons for the stringent limitations on data collection and the localization mandate in the Guidelines are:

• Due to the excessive amount of personal information that DLAs and LSPs collect from borrowers (also including by reputable fin techs) that offer digital lending, some apps even require users to grant permissions to access personal data like their location, camera, and contacts even though those permissions are not necessary for the services that the digital lending platforms offer.

• The flagrant mishandling of client information by a number of these DLAs/LSPs. According to news reports, cybercriminals in India allegedly used more than 300 digital lending apps to harass borrowers and obtain user data.

5. Mandatory due Diligence Requirements

According to the Guidelines, Real Estate Advisors (REs) are required to make sure that any lending made through their DLAs or LSPs is reported to the Credit Information Companies (CICs). This is true regardless of the type of loan or its duration; whether it is through a merchant platform, short-term, secured or unsecured credit, or deferred payments, the REs are responsible for reporting all lending to CICs. Before collaborating with an LSP for digital lending, REs must

perform comprehensive and enhanced due diligence, covering the LSP's technical capabilities, data privacy policies, storage systems, fairness in dealing with borrowers, and capacity to adhere to laws and regulations. Additionally, REs are accountable for conducting regular reviews of LSP behavior and guide them efficiently and keep an overview while they act as recovery agent.

These due diligence requirements were put in place in response to several fintech lending apps that employ severe and predatory lending and recovery practices. If REs are forced to thoroughly vet LSPs before partnering with them, the number of these lenders operating in the digital lending space could be significantly decreased, according to RBI.

BNPL Industry Concern vis-à-vis the Guidelines

The RBI circular on Prepaid Payment Instruments ("PPIs") and credit lines, published in June 2022, forbade the loading of non-bank PPIs, such as prepaid cards and wallets, from credit lines prior to the guidelines on digital lending in September of that same year. As we all know, credit lines are pre-approved borrowing amounts given by banks or non-bank financial institutions (NBFCs). If the credit falls within the pre-approved borrowing limits, individuals and businesses can access credit at any time without requiring additional approval.

The RBI's Master Direction on PPIs [7](dated September 24, 2021) highlights that PPIs, including e-wallets, can only be loaded and reloaded with cash or debits to a bank account and credit and debit cards. PPIs cannot be loaded through credit lines. The RBI's restriction on credit lines affected a number of "Buy Now Pay Later" (BNPL) platform providers because these platforms' main source of revenue came from providing credit to their users via non-bank issued PPIs loaded with pre-approved credit lines.

The RBI's Master Direction on PPIs emphasizes that PPIs cannot be loaded through credit lines and that PPIs, such as e-wallets, can only be loaded and reloaded using cash or debits to a bank account and credit and debit cards. A number of "Buy Now Pay Later" (BNPL) platform providers were impacted by the RBI's restriction on credit lines because the primary business

[7]Master Direction – Reserve Bank of India (Securitizations of Standard Assets) Directions, 2021 (Updated as on December 05, 2022), RBI/DOR/2021-22/85 https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12165(Accessed 23 November 2023)

model of these platforms was to offer credit to their users through non-bank issued PPIs that were loaded using pre-approved credit lines.

Because the credit lines were already pre-approved and the borrowers didn't need additional approval to use the BNPL service, loans could have been provided to them instantly or within minutes of their request prior to the restriction. Due to the RBI's restriction on credit lines, BNPL companies are now required to switch to a new model of loan sanctioning for each and every lending transaction that a borrower completes on the platform. Therefore, this new model necessitates that the loan be authorized, disbursed, and then loaded into the PPI at each instance, lengthening the process and ultimately defeating the purpose of Fintech.

A number of these BNPL platforms have changed their business models as a result of this new, laborious process. In order to ensure that there was no pass-through of loan disbursal or repayment through the BNPL platform account or any other intermediary account, the RBI Guidelines also required changes to be made by the BNPL platforms. The credit lines circular and the Guidelines have combined to create a double whammy that makes it nearly impossible for BNPL companies to operate in their previous form. Due to such drastic measures, a number of these fintech businesses have had to take a hard turn in their business model and in some cases even wrap up their business.

Conclusion

The BNPL Gross Merchandise Value in the India will increase from US$12.2 billion in 2022 to reach a staggering US $26.1 billion by 2028**.** According to reports BNPL will overtake credit card in terms of market adoption with the number of BNPL users are estimated to be 10-15 million already and are expected to grow as much as 10 times to 100 million by 2026. Hence India is galloping in the Fintech industry and although putting a leash of regulation is necessary it has to be ensured that the leash should not choke the neck of the Digital India dream.

The RBI Guidelines cover consumer and data protection in great detail, however, for their implementation to be successful, industry-specific issues still need to be clarified. Industry players sincerely hope that RBI will provide more elucidation on the Guidelines, especially concerning the exemptions pertaining to FLDG offerings. Clarification of this kind is essential because it will allow the Fintech sector to design the best possible model for profitable

operations that conforms to the law. One way to encourage REs to lend digitally through LSPs and DLAs is to develop models related to FLDGs, so this is a relevant factor for the growth of digital lending as well as inclusive growth.

Hence a perfect harmony has to be maintained with a Regulation but keeping in sight the needs and requirement of the growing industry has to be prioritized as well and constant feedback needs to be taken from these Industries of their requirement, as they are growth engines of economy to propel the dream of $5 Trillion economy of India by 2025.

REGULATORY SANDBOXES AND REGULATORY BODIES IN INDIA: A PLAYGROUND FOR INNOVATIONS IN FINTECH SECTOR

- ***Shreyansh Harshit***[1]

Abstract

Recently, Financial Technologies (FinTech) have experienced a boom and pragmatically changed financial services and their delivery to the populace in India. Further, it is expected to grow USD 1.3 Trillion by 2030[2]*. The contribution made by the FinTech companies in this sector to new milestones is laudable. In 2021 the Reserve Bank of India (RBI) came up with an enabling framework for a Regulatory Sandbox (RS) to provide regulatory guidance and new opportunities for consumers. RS promotes innovation and acts as a point of communication to regulatory bodies which prevents regulatory arbitrage and lag. The future of this sector is contingent upon the efficient functioning of RS. Regulations determine the efficiency of the RS program. In this nurturing field, the regulatory bodies have a very important role in regulating the RS very shrewdly to harness the benefits attached thereto. This article tries to study the background and reasoning behind the enactment of RS in India and its contribution to changing the FinTech sector. This article is an attempt to throw light on the impact of regulation in the nurturing field of FinTech and expounds on the role of bodies as guardians to foster them. The article, after studying the available literature and considering the debate of favoring rule-based regulation and principle-based regulation, tries to establish and justify that to tackle the imposing challenges the regulators should come up with a blend of both rule and principle-based regulations.*

Keywords: *Regulatory Sandbox, FinTech, Regulatory Body, Regulations, Playground for Innovation.*

[1] Third Year, Chanakya National Law University. Gmail : shreyanshharshitcnlu@gmail.com

[2] Jatinder Handoo, *FinTech SRO: The Paradigm Shift in FinTech Regulation in India*, ETBFSI, (Oct. 27, 2023, 08:00 AM), https://bfsi.economictimes.indiatimes.com/blog/fintech-sro-the-paradigm-shift-in-fintech-regulation-in-india/104740095 (last visited on 13-11-2023).

I. Introduction

The increment in internet coverage and access to smartphones in India further accompanied by initiatives such as Digital India and 'less-cash' culture has led to a boom in FinTech. FinTech has huge potential to extend the benefits of financial services in India considering its population and people who are left uncovered by the traditional banking system. FinTech in the Indian context has not been defined by the RBI. However according to the inter-regulatory Working Group (WG) Report it "*refers to the technological start-ups that are emerging to challenge traditional banking and financial players and cover an array of services, from crowdfunding platforms and mobile payment solutions to online portfolio management tools and international money transfers"*[3]. According to the Financial Stability Board of the Bank for International Settlement, "*FinTech is technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services"*[4]. Simply, it means the inclusion of technology in financial services thereby expanding the benefits to financial sectors and consumers. It has led to multiple financial innovations in India. Innovation is very necessary for a nation to compete in the increasingly competitive market[5]. There has been many innovations and development in the field of FinTech some examples of innovations are Automated Teller Machines, National Electronic Funds Transfer (NEFT), Risk Management Products, Right Time Gross Settlement (RTGS), Mobile Banking, Bharat Interface for Money (BHIM), Unified Payments Interface (UPI), Phone Pe, Google Pay, etc.[6]

These innovations are the outcome of RS inter alia, which started gaining traction after its creation in the United Kingdom (UK) by the Financial Conduct Authority in 2016[7]. The RS provides a small platform for the products or services by innovators to test in a controlled

[3]*Report of the Working Group on FinTech and Digital Banking*, RESERVE BANK OF INDIA (Nov. 23, 2017), https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF (last visited on 21-11-2023).

[4] Financial Stability Board defining FinTech, https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech/ (last visited on 21-11-2023).

[5] Ram Singh & Rohit Bansal, *Financial Innovation in India: A Conceptual Study*, RESEARCHGATE, Jan. 2020, at 220, 220.

[6]*Regulatory sandbox lessons learned report*,FINANCIAL CONDUCT AUTHORITY, (Oct. 2017) https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf (last accessed on 13-11-2023).

[7] Giulio Cornelli et al., Regulatory *Sandboxes and Fintech Funding: Evidence from the UK*, BANK FOR INTERNATIONAL SETTLEMENTS (Nov. 2023), https://www.bis.org/publ/work901.pdf (last visited on 13-11-2023).

regulation. The test tries to assess the benefits and demerits of the products or services. Also, RS provides a reality check on the innovative product or service before launching it in the public market[8]. The main objective of RS is to foster innovation in FinTech by allowing the testing for their products or services[9] and direct evidence of risks and benefits. Moreover, RS also provides a platform to check the regulatory framework which is made by various independent regulatory bodies in India.

The RS are generally regulated by regulatory bodies like RBI, the Security and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority of India (IRDAI), and the Pension Fund Regulatory and Development Authority (PFRDA)[10]. Operating Procedure for Inter-Operable RS[11] to facilitate the testing of products or services falling within the ambit of more than one regulatory body[12].

In the time of growing technologies and advancement in FinTech especially, it becomes crucial and challenging simultaneously to come up with a set of regulations covering all the RS within its ambit. The article will analyze the existing regulations and provide solutions and recommendations to give a facilitative and flexible playground to FinTech companies in the RS program. The article will discuss whether rule-based regulations or principle-based regulations are good for FinTech RS. The article will also discuss and argue about the importance of having a uniform regulatory framework among various sectors for RS in India. Section II will talk about RS and its purpose and how RS reduces the burden of Regulatory Bodies in framing effective regulations. Section III will discuss about regulatory bodies and the regulatory framework for FinTech sandboxes in India. Further, section IV will discuss, identify challenges, and provide

[8]*Enabling Framework for Regulatory Sandbox*, RESERVE BANK OF INDIA (Oct. 08, 2021), https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/ENABLINGFRAMEWORK815099571ACC411F8B9C0EB6534E681F.PDF (last visited on 17-11-2023).

[9]*Supra* note 6.

[10]*Framework for Regulatory Sandbox*, INTERNATIONAL FINANCIAL SERVICES CENTRES AUTHORITY, (2020), https://ifsca.gov.in/Document/Legal/ifsca-circular-regulatory-sandbox_new19102020084227.pdf (last visited on 17-11-2023).

[11]*Inter-operable Regulatory Sandbox: Standard Operating Procedure*,RESERVE BANK OF INDIA, https://rbidocs.rbi.org.in/rdocs/Content/PDFs/IORS121020222D6F89A76B53488585EC6F0CF52A38AC.PDF &Standard Operating Procedure for Inter-operable Regulatory Sandbox, Securities and Exchange Board of India, (Oct. 12, 2022), https://www.sebi.gov.in/media/press-releases/oct-2022/standard-operating-procedure-for-inter-operable-regulatory-sandbox-iors-_63948.html (last visited on 13-11-2023).

[12] Anushka Sengupta, *Explained: Interoperable digital platforms, RBI and SEBI's SOP*, ETBFSI, (Oct. 17, 2022, 08:00 AM), https://bfsi.economictimes.indiatimes.com/news/fintech/explained-interoperable-digital-platforms-rbi-and-sebis-sop/94902339 (last visited on 13-11-2023).

solutions and recommendations for regulations for innovation in FinTech to improve the RS program. Lastly, the article will conclude with some recommendations and argue that principle-based regulations blended with rule-based regulations are good for identified challenges in the regulation of FinTech RS.

II. Regulatory Sandbox and its Purpose

1. Background and Definition

FinTech in India has recently witnessed huge growth in its adoption and usage by the general populace of the country. The surge in FinTech services is due to the growth and potential of FinTech firms. Also "*India has been at the forefront of this revolution*" as stated by Shri Shaktikanta Das in his keynote address[13]. Moreover, India has also been ranked second in FinTech adoption at the adoption rate of 52 percent[14]. The RBI and Digital India initiative has encouraged the adoption of a less cash society which has resulted in the development of various national payment infrastructures such as Immediate Payments Service (IMPS), BHIM, UPI, Bharat Bill Pay System (BBPS) and Aadhar-enabled Pay System (AePS)[15]. The RBI has also introduced specific regulations or policy approaches in the payments, lending, retail banking, and financial management segments of FinTech[16]. The developments in FinTech show its dynamics of rapid evolution within a short period. As a response to the rapid evolution of FinTech, the WG committee was set up by RBI in July 2016[17] to provide recommendations in the FinTech field

[13]*Opportunities and Challenges of FinTech*, RESERVE BANK OF INDIA, (Mar. 25, 2019), https://rbidocs.rbi.org.in/rdocs/Speeches/PDFs/GSFNA250319AD0EE1F30EB746028A177251138EC297.PDF (last visited on 14-11-2023).

[14]*Global FinTech Adoption Index 2019*, ERNST & YOUNG GLOBAL LIMITED, (Oct, 2019) https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-global-fintech-adoption-index-2019.pdf?download (last visited on 14-11-2023).

[15]*Supr*a note 11, ¶ 5 (last visited on 14-11-2023).

[16]*RBI grants "in-principle" approval to 11 Applicants for Payments Banks*, RESERVE BANK OF INDIA, (Aug. 19, 2015), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=34754; Vishwanath Nair & Vivina Vishwanathan, *RBI Proposes P2P Lending Regulations*, MINT, (Apr. 28, 2016, 01:58 PM), http://www.livemint.com/Industry/Vx9iwySoYwxHxfIsPq2r1L/RBI-proposes-regulatory-framework-for-P2P-lending-platform.html; *RBI releases Names of Applicants of Small Finance Banks and Payments Banks*, RESERVE BANK OF INDIA, (Feb. 04, 2015), https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=33164 &*RBI floats Draft Regulatory Framework for Account Aggregator Companies to facilitate Consolidated Viewing of Financial Assets Holdings*, RESERVE BANK OF INDIA, (Mar. 03, 2016), https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=36394 (last visited on 14-11-2023).

[17] RBI sets up Inter-regulatory Working Group on Fin Tech and Digital Banking, Reserve Bank of India, (July 14, 2016), https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR1148A4D9E65B13F44AA8E359826ED8610FD.PDF (last visited on 14-11-2023).

and to review the regulatory framework and responses to the dynamics of this field. The committee recommended introducing an appropriate framework for RS[18]. With the growing popularity and affordability of FinTech services in India innovations and RS regulations have become very crucial for its development. The sandbox has been defined in the report by WG as "*live or virtual testing of new products or services, in a (controlled) testing environment, with or without any regulatory relief*"[19]. This is not a new concept in the world, several countries like Australia, Canada, Denmark, the UK, Singapore, the Netherlands, US have also established the RS program.

2. Purpose of RS

The purpose of the RS is to foster growth and increase innovation by companies. It also includes the protection of the customers' interest and flexibility for the innovative companies[20]. Sandbox enables companies in regulated environments to test their creativity in real-life market scenarios. It provides a boost to the startup companies especially to come up with their new product or services to improve the existing conditions of the market. Most of the innovation in FinTech is brought by startup companies. RS has been a major contributor in developing new products or services which has pragmatically changed the traditional financial system of the country. Some successful RS programs include PayTM, PolicyBazaar, Kenko, Acko, Bharatpe, PhonePe, Zerodha, Groww, and many more. With these new FinTech products or services, the delivery of financial services like banking, money transfer, stock purchase, and trading has become easy.

However, to what extent the purpose of RS be achieved is contingent upon the fact that which kind of regulations are imposed by the concerned regulatory body. The regulation determines the flexibility, time, security to consumers, and eligibility criteria. As the find is very dynamic and growing rapidly day by day it becomes very challenging to come up a hard and fast regulations. Hence, the regulation must be enacted shrewdly to harness the benefit of RS effectively.

[18]*Supra* note 2, at 3.
[19]*Supra* note 2, ¶ 4.2.2.
[20]*Report of Committee on Regulatory Sandbox in insurance sector in India*, INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA, (Feb. 05, 2019), https://irdai.gov.in/document-detail?documentId=390684 (last visited on 14-11-2023).

3. RS reducing regulatory bodies' burden

FinTech changes the functioning of the financial market. The impact of these new technologies is very influential in society. It might bring change positively and also negatively such as cyber-crimes. The RS has been also developed in response to FinTech regulation[21]. The regulatory framework for RS must be adaptive considering the continuity and evolving nature of this field to avoid regulatory gap and arbitrage. Communication between the body and the market is very essential in understanding the existing reality of the market to frame regulations accordingly. The RS program serves as the point of communication[22]. It communicates the benefits and the risks associated with it. The RS prevents information asymmetries between regulators and entities[23]. The RBI enabling framework also encourages innovation where governing regulations are absen*t* to regulate effectively[24]. In the RS program, the regulators also come to know the gap between regulation and the real market, challenges, difficulties, data security, inconveniences, privacy, problems, and security issues due to new technologies. After observing such lacuna, the regulators will then analyze and rectify such regulations and enact new regulations, if needed, to overpower those identified lacuna accordingly. In India, these regulators are independent governmental regulatory bodies.

III. Regulatory bodies and their framework for RS

The regulatory framework for FinTech sandboxes in India is made by independent regulatory bodies. The framework is very crucial for the future of FinTech industries in India. Post-1990s, the role of regulatory bodies became very crucial to ensure a free and fair market. Their role includes nurturing and parenting of the private sectors in their defined ambit. They are independent governmental bodies empowered to come up with rules, regulations, circulars, etc. to serve and protect the public interest, to prevent market failure, etc.[25] They (RBI, SEBI, and IRDAI) have made their regulations for RS.

---

[21] Simona HesekovaBojmirova, *FinTech and Regulatory Sandbox - New Challenges for the Financial Market. The Case of the Slovak Republic*, 12 JURIDICAL TRIB. 399, 400 (2022).
[22]*Id.*
[23]Zetzsche et al, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, 23 FORDHAM JOURNAL OF CORPORATE & FINANCIAL LAW 31, 69 (2017).
[24]*Supra* note 7, ¶ 5.
[25] Vidhika Sharma et al., *Audit of Regulatory Bodies*, REGIONAL TRAINING INSTITUTE, JAMMU, (Mar. 18, 2019) https://cag.gov.in/uploads/media/GroupIV-RegulatoryBodies-20200518224004.pdf (last visited on 13-11-2023).

1. Frameworks and guidelines

The RS Enabling Framework has been issued by the RBI on 13th August 2019[26]. The objective of the framework is to "*foster responsible innovation in financial services, promote efficiency, and bring benefit to consumers"*[27]. The eligible FinTech companies apply for RS. Thereafter, they continue with testing which lasts for a maximum of sixteen weeks and which may be extended or discontinued at any time at the discretion of RBI. The discontinuation can be done, if the sandbox entity- does not achieve its intended purpose, is unable to fully comply with regulations, and acts not in the best interest of the consumers[28].

The framework targets FinTech companies fulfilling eligibility criteria to encourage innovation. The eligibility criteria focus on the area where governing regulation is absent, the need for easing the regulations temporarily, and proposed innovation easing significantly the delivery of financial services[29]. However, the RS is restricted to only certain fields of FinTech. It does not cover fields like credit registry, credit information, cryptocurrency, chain marketing services, etc.[30] Efforts must be made to cover more fields under RS programs.

2. Regulations for innovation in FinTech RS.

Hitherto it has become important to regulate the sandboxes carefully to maintain the balance between the innovation and public interest. The regulation must not be restricted only to certain indicative products or technologies as enabled by RBI[31]. The rush to regulate the sandbox may be a mistake[32]. Effective regulation in the field of FinTech is very crucial for innovation hubs. The regulation has to favor the innovative FinTech startup but in the garb of RS, they should not be given substantive relaxation under the RS program. The program should be continuously monitored by the body to check the effectiveness of regulation so that it does not unreasonably affect the healthy competition in the market. Hence, there must be active regulation by regulatory bodies. The WG report has cautioned against two caveats, one being barriers for newcomers

[26]*Enabling Framework for Regulatory Sandbox*, RESERVE BANK OF INDIA, (Aug. 13, 2019), https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR4172205C8483FA44CD2846079912DD77AB5.PDF (last visited on 13-11-2023).
[27]*Supra* note 7, at 2.
[28]*Supra* note 7, ¶ 6.6.
[29]*Supra* note 7, ¶ 5.
[30] Supra note 7, ¶ 6.3.
[31]*Supra* note 7, ¶ 6.1.3.1-6.1.3.2.
[32]*Supra* note 43, at 349.

affecting innovation and the other being, undue favor to newcomers in relaxing regulations[33]. The regulations have not only an impact on the competition between startup companies but also between startup companies and already existing firms[34]. Hence, the role of regulation is not only limited to providing a playground for startup companies but also for all participants, be it existing or new startups, to maintain innovation, security, and healthy competition in the financial market.

IV. Challenges

The scenario of existing regulations has been encapsulated in Section III.*1*. As observed earlier there are separate but similar regulations made by the concerned regulatory body and separate regulations for interoperability by RBI and SEBI. Hence, there is clarity in regulation among various bodies. The bodies have defined their eligibility criteria clearly and entry and exit strategies that can maintain regulatory certainty. Regulatory certainty is not only limited to such criteria and strategies but also to consumer awareness, financial literacy, and security of data inter alia. However, there are some challenges in front of regulatory bodies while enacting regulations.

1. Regulatory lag

As stated by Hesekova "*FinTech causes dynamic changes within the financial market, not only by making new business models and products conditional, but also by changing the functioning of the financial market. The right setting of FinTech regulation while maintaining the full potential of new technologies is thus a considerable challenge for legislators*"[35]. The first challenge is that the field of FinTech is very dynamic and still growing day by day which makes it difficult for the job of bodies to come up with regulations or even hard and fast regulations to cover all the aspects. It should be effective and secure in achieving the objective behind the establishment of RS. To remain effective, the regulations must adopt the evolving landscape of FinTech. It should try to avoid regulatory lag and loopholes giving the benefit of regulatory arbitrage to the companies. Regulatory arbitrage means "*the practice of structuring activities or*

[33]*Supra* note 2, ¶ 6.1.4.
[34]*Id.*
[35]*Supra* note 20, at 400.

business functions to gain from the differences in regulations or gaps, specifically from cross-country differences in regulations."[36]

Furthermore, in the case of F.T.C. v. Wyndham Worldwide Corp.[37] The Third Circuit Court of Appeals while upholding the authority of the Federal Trade Commission to regulate cybersecurity practices underscored the huge importance of regulatory adaptability to tackle the emerging risks in the digital modern world. Another case of United States v. Zaslavskiy[38] showcased the need for regulatory frameworks to keep pace with innovation in financial technology such as cryptocurrencies and blockchain.

2. Inflexibility

The problem in this quandary is that if the regulator comes up with such regulation, the access to RS will be restricted to the known or even assumed products or services by limited participants as it is the regulation that determines the eligibility criteria and entry and exit strategies. Further, flexibility in terms of regulation is required to enable good and healthy competition in the RS program. The second challenge that appears is how much flexibility should be given to participants. The same thing was cautioned by the WG report that there should not be undue favor in the name of innovation. The flexibility in regulations is very important to enable flexibility in the playground for innovation. At the same time, the interest and safety of consumers should not be overlooked. It is very difficult to come up with a perfect line of demarcation with a perfect balance among these challenges.

Furthermore, in the landmark case of Securities and Exchange Commission v. W J Howey Co[39] The United States Supreme Court emphasized the need for regulatory flexibility in order to address innovation in financial services and products.

3. Balancing innovation and consumer interests

[36]*What Is Regulatory Arbitrage,*WALL STREET MOJO, https://www.wallstreetmojo.com/regulatory-arbitrage/ (last visited on 17-11-2023).
[37]F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015).
[38] United States v. Zaslavskiy, 1:17-cr-00647 (E.D.N.Y. Sept. 11, 2018).
[39] Securities and Exchange Commission v. W J Howey Co, 1946 SCC OnLine US SC 95.

These resolutions have been designed to balance innovation with consumer protection and financial stability in the following manner. Firstly, it requires every applicant to satisfy eligibility criteria to apply to participate in the RS program[40]. The application processes involve the consideration of viability, innovation, and potential risks and benefits for the consumers. Secondly, it requires disclosures[41], indemnification for liabilities, consent mechanisms, ensuring the fulfilment of any existing obligations to the customers before the exit or discontinuation of the RS[42], and customer privacy and data protection[43]. The compliance of these provisions by FinTech companies will protect the interests of consumers and the innovation of FinTech as well. Some successful participants of the RS program of different regulators include the approval of BharatPe[44] and PayTM[45] from RBI, Acko, and PolicyBazaar from IRDAI[46] and Zerodha[47] and Groww[48] from SEBI. These unique approaches by the FinTech companies have fostered innovation with the help of the regulations made by the concerned regulatory bodies. The role of regulation is very crucial in facilitating innovation. It is very challenging to set the tone of regulation as safe for consumers as well as facilitating innovation. As Brummer has observed the "*regulatory and market disruptions overlap".*[49]Dierdre Ahern has further stated that many regulators use the 'wait and see' approach to calculate the costs and benefits of innovations[50]. Further, the given example of EU institutions undergoing information gathering and monitoring

[40] Supra note 7, ¶ 6.5.
[41] Supra note 7, ¶ 9.
[42] Supra note 7, ¶ 6.6 (d) & ¶ 6.8.2.
[43] Supra note 7, ¶ 6.2.
[44] Malvika Maloo, *BharatPe receives in-principle nod from RBI for online payment aggregator*, MINT, (Jan. 10, 2023, 06:42 PM), https://www.livemint.com/companies/news/bharatpe-receives-in-principle-nod-from-rbi-for-online-payment-aggregator-11673355879459.html (last visited on 14-11-2023).
[45] Pranav Dixit, *RBI allows Paytm Payments to continue online Payment Aggregator business as it awaits govt approval*, BT, (Mar. 28, 2023, 3:04 AM), https://www.businesstoday.in/latest/corporate/story/rbi-allows-paytm-payments-to-continue-online-pa-business-as-it-awaits-govt-approval-374876-2023-03-26 (last visited on 14-11-2023).
[46] Girish Shetti, *Exclusive: Acko&PolicyBazaar get IRDAI approval under Sandbox Regulatory Program*, TECH PLUTO, (July 31, 2020), https://www.techpluto.com/exclusive-acko-policybazaar-get-irdai-approval-under-sandbox-regulatory-program/ (last visited on 14-11-2023).
[47]*Zerodha gets Sebi's approval to set up an AMC*, ET, (Sep. 01, 2021, 09:32 PM), https://economictimes.indiatimes.com/tech/startups/zerodha-gets-sebis-approval-to-set-up-an-amc/articleshow/85838821.cms (last visited on 14-11-2023).
[48] Jyoti Banthia, Groww Mutual Fund receives SEBI's go-ahead for launching first index fund, TH Business Line, (Sep. 07, 2023, 07:25 PM), https://www.thehindubusinessline.com/markets/groww-mutual-fund-receives-sebis-go-ahead-for-launching-first-index-fund/article67280768.ece (last visited on 14-11-2023).
[49] C Brummer, *Disruptive Technology and Securities Regulation*, 84 FORDHAM LAW REVIEW 977, 980 (2015).
[50] Deirdre Ahern, *Regulators Nurturing Fintech Innovation: Global Evolution of the Regulatory Sandbox as Opportunity-Based Regulation*, 15 INDIAN J. L. & TECH. 345, 378 (2019).

of business despite rushing to regulate in FinTech space[51]. The approach of Indian regulators must be considerate of such views. Hence, the burgeoning field of FinTech must be regulated carefully to harness the benefits of innovative startups.

Furthermore, in the case of Consumer Fin. Prot. Bureau v. TransUnion[52] The Fifth Circuit Court of Appeals, while upholding the constitutionality and authority of the Consumer Financial Protection Bureau to enforce the federal consumer protection laws, highlighted the need for important robust regulatory oversight in the emerging FinTech area.

V. Conclusion

The traditional financial sector was dominated by the Banks. Now, the financial sector is witnessing a paradigm shift in its working and delivery of services. FinTech companies have brought a revolutionary change in the financial sectors through innovative products or services. The playground for innovation in this revolution is enabled by the RS program. The RS program is a very new concept in India and has huge potential to expand further. This line article has discussed the concept of RS and the role of regulatory bodies in regulating them to provide a playground for innovation. The article has explained that RS gives a common playground to both companies and regulatory bodies to check the innovative product or service and regulations in the real market respectively.

The RS is mutually beneficial for companies and bodies. Further, the role of regulatory bodies is not only limited to enacting apt regulations for governing the RS but also its active participation in this emerging field to facilitate innovation while protecting the interests of consumers. After considering and identifying challenges in the existing regulatory framework by various regulators in India, the article has expounded that the approach of regulatory bodies while enacting regulations must be amenable to the changes and flexible enough to facilitate innovation by companies.

[51]*FinTech Action Plan: For a More Competitive and Innovative European Financial Sector*, EUROPEAN COMMISSION, (2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0109 (last visited on 17-11-2023).
[52]Consumer Fin. Prot. Bureau v. TransUnion, 22 C 1880 (N.D. Ill. May. 23, 2023).

Furthermore, the regulations should not also consider the competition between participants in RS programs, it should also maintain healthy competition between operating companies and participating companies in RS. In this line, the article further expounded that the blend of rule and principle-based regulation will suffice in this situation by regulating more in areas having higher risk which affects market and consumer safety, and less in areas having lesser risks like defining eligibility criteria, time-period and application of RS to other products or services. Such flexible regulation will ensure that the RS program is not being used as a tool to defeat good and healthy competition in the real market by unduly favoring the participating companies in RS. In all this process what is ultimately required the most is the need for collaboration from both sides that is between the FinTech companies and regulatory authorities to drive this burgeoning sector to its new zenith.

VI. Way forward and Suggestions

The principle of fairness and equality must be incorporated while enacting regulations for sandboxes concerning the aforementioned tradeoffs[53]. Presently, the Indian financial market is highly regulated and RS participants have noted that regulations have become rule-based as opposed to principle-based regulation[54]. Both types of regulation have their benefits and risks. The former emphasizes compliance with regulations and gives clarity on what is allowed and what is not while the latter focuses on the outcome by giving companies more discretion in terms of control, measures, and procedures[55]. The latter has the risk that there will be uncertainty and inconsistent implementation of the regulations as it depends on the skill set of the company to set the measures and procedures to achieve the set outcomes.

1. Resolving flexibility, regulatory gap, and innovation.

The problem of regulatory arbitrage inter alia. The risks of data protection and the privacy of consumers are very serious and they cannot be compromised by leaving it at the discretion of the companies to protect the same by their regulations. Hence, the need of the hour is that the regulations must be a blend of both rule and principle-based regulation. The blend of rule and

[53] *Supra* note 43, at 361.
[54] Shashidhar K.J., *Regulatory Sandboxes: Decoding India's Attempt to Regulate Fintech Disruption*, 361 ORF ISSUE BRIEF 1, 11 (2020), https://www.orfonline.org/wp-content/uploads/2020/05/ORF_Issue_Brief_361_Fintech.pdf (last visited on 17-11-2023).
[55] *Id*.

principle-based regulation will suffice in this situation by regulating more in areas having higher risk which affects market and consumer safety and less in areas having lesser risks like defining eligibility criteria, time-period, and application of RS to other products or services. This kind of regulation will be more flexible and innovation-friendly. The challenge here arises when the rule or principle-based regulation should be used. It would be decided on the basis of risks involved in various programs or specific areas within the program. Rule-based regulation shall be enacted for programs having higher risks which will provide clarity, duties, and responsibilities to the participants. The rule-based regulation provides a clear idea about what is allowed or not. Furthermore, the area of less risk can be regulated by a principle-based regulation. The regulation of this kind will create a more creative playground for innovation by providing flexibility as well as rigidity.

It is evident and observed that RS helps bodies check the regulations in real time to check their effects on the market. This is the live testing of regulation. The analysis after the program seeks to work on the appropriateness of regulatory framework to encourage innovation in the playground. The World Bank Document mentions that "*Sandboxes offer considerable value to policymakers seeking to increase their understanding and capacity to facilitate and regulate a range of fintech innovations*"[56]. Furthermore, in the same document, it has been stated that "*About 73 percent of regulators reported that implementing a sandbox contributed to building their capacity around fintech, and about 85 percent reported that it helped them to assess the appropriateness of their legal or regulatory frameworks.*"[57] This data establishes that the value of regulations will improve with the implementation of the sandbox itself.

Moreover, the RS program of the Monetary Authority of Singapore has guided many firms[58]. Hence, the regulations must be enabling and facilitating while having a mixture of flexibility and some rigidity as mentioned above. The playground enables learning for both the participants and the regulators. Hence, the approach must be flexible. Furthermore, the approach of various

[56]*Global Experiences from Regulatory Sandboxes*, WORLD BANK GROUP, (2020), https://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf (last visited on 21-11-2023).
[57]*Id.*
[58]*Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offces, Regulatory Sandboxes, and RegTech* , UNITED NATIONS SECRETARY-GENERAL'S SPECIAL ADVOCATE FOR INCLUSIVE FINANCE FOR DEVELOPMENT, (2019), https://www.finextra.com/finextra-downloads/newsdocs/unsgsa_report_2019_final-compressed.pdf (last visited on 21-11-2023).

regulatory bodies in India must be to come up with a single and uniform regulation where interoperability between various sectors is concerned. This step will remove the regulatory compliance hurdle and conflicts between the regulations which consumes a lot of time. Therefore, the creation of a facilitative playground for innovation would achieve the new zenith.

DATA PROTECTION, REGULATIONS, AND CYBERSECURITY: AN IMPACT ON MERGERS AND ACQUISITIONS AND LEGAL RAMIFICATIONS

- ***Aniket Jadhav***[1]

Abstract

The article delves into the critical intersection of cybersecurity, data protection regulations, and their profound impact on mergers and acquisitions (M&A). In light of escalating cyber threats and the transformative impact of digitalization, meticulous cybersecurity due diligence is paramount for businesses involved in M&A transactions. This research underscores cybersecurity's integral role in the due diligence process, emphasizing its crucial role in uncovering potential risks, exposures, and liabilities.The study advocates for sustained emphasis on cybersecurity to It outlines the steps in cybersecurity due diligence, encompassing evaluation of internal IT infrastructure, assessment of the target firm's information security, and the implementation of post-merger security protocols to bolster cyber resilience. Moreover, the research explores the evolving legal landscape, particularly in India, where data privacy and cybersecurity are increasingly pivotal in M&A. It delves into the existing legal framework, including the Information Technology Act and Rules, alongside anticipated legislation such as the Personal Data Protection Bill of 2019. The conclusion underscores the importance of a comprehensive, strategic, and forward-looking cybersecurity approach to ensure M&A transaction success. As regulatory environments evolveorganizations are compelled to adapt, with the recent introduction of the Data Protection Act of 2023, adding complexity. Ultimately, the research stresses on some indispensable components for successful mergers and acquisitions in the ever-evolving digital ecosystem.

Keywords: *Cybersecurity, Mergers and Acquisitions (M&A), Due Diligence, Digital Transformation, Cyber Resilience.*

[1] Advocate, Bombay High Court. Gmail: law.aniket@gmail.com

Background and Significance

Cybersecurity: Refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact. Cybersecurity aims to protect individuals' and organizations' systems, applications, computing devices, sensitive data and financial assets against simple and annoying computer viruses, sophisticated and costly ransomware attacks, and everything in between.[2] In recent years, significant IT trends such as increased cloud computing adoption, growing network complexity, the rise of remote work and BYOD programs, and the proliferation of connected devices have brought about substantial business advantages and societal progress. However, these developments have also expanded the attack surface for cybercriminals. A recent study reveals a global cybersecurity worker gap of 3.4 million, highlighting the challenge of filling the increasing demand for cybersecurity professionals.[3] In response, resource-constrained security teams are prioritizing the development of comprehensive cybersecurity strategies. These strategies incorporate advanced analytics, artificial intelligence, and automation to enhance the effectiveness of cyber threat defence and mitigate the impact of cyberattacks.

Due Diligence: Due diligence is a comprehensive process involving the verification, investigation, or audit of a potential deal or investment opportunity. Its purpose is to confirm all pertinent facts and financial information and to validate any aspects raised during an M&A deal or investment process. This thorough examination is conducted prior to the deal's closure, offering the buyer assurance regarding the nature and quality of what they are acquiring.

In the context of mergers and acquisitions, a thorough due diligence process is crucial before any transactions take place. This process involves a comprehensive review and audit of the businesses involved to ensure optimal decision-making and maximize added value. Failure to complete this due diligence is a key reason for M&A failures. The goal is to understand synergies and scalability potential post-merger/acquisition. The process identifies internal and external factors posing risks and focuses on key profitability drivers. A careful analysis of employees, processes, and patents is conducted to gain a clearer understanding of the business

[2]IBM. (2023). What is cybersecurity? https://www.ibm.com/topics/cybersecurity.
[3]Platsis, G. (2023, February 3). Bridging the 3.4 million workforce gap in cybersecurity. Security Intelligence. Retrieved from https://securityintelligence.com/articles/bridging-workforce-gap-cybersecurity

landscape. Scenario planning is employed to assess risks and opportunities, providing richer insights than traditional balance sheet analysis.

The Intersection of Digital Transformation and Cybersecurity in M&A

Digital transformation has been a driving force in mergers and acquisitions (M&A) for the past decade, and its momentum is expected to intensify in 2024. Businesses in various sectors recognize that their survival and competitiveness depend on embracing technology. The tech sector, in particular, is anticipated to see ongoing M&A activity, with both established companies and start-ups strategically acquiring to strengthen their positions. To remain competitive, companies are advised to consistently invest in digital transformation. Optimism prevails regarding M&A transactions in technology, energy, healthcare, life sciences, and smart manufacturing. Whether taking the role of acquirer or being acquired, possessing robust digital capabilities is deemed a strategic advantage.[4]

In recent times, business leaders, boards, and internal audit committees have increasingly recognized the importance of cybersecurity, leading to heightened investments in various areas of organizations to enhance cyber assurance and defences. Despite the global economic downturn triggered by the COVID-19 pandemic, geopolitical tensions, and other unforeseen circumstances, mergers and acquisitions (M&A) continue to be prevalent across various industry sectors. Despite fluctuations in transaction volumes, M&A and divestments have become standard practices in the modern business landscape.

Every year witnesses thousands of deals taking place globally across different industries. While each transaction is unique, a consistent factor is the growing significance of cybersecurity in M&A to mitigate risks associated with these transactions. As an integral component of the due diligence process, cybersecurity plays a pivotal role in revealing potential cyber risks, exposures, and liabilities for organizations. It serves as valuable input to assess the cost of remediation, impacting the valuation of a deal and potentially altering its course. These assessments are

[4]Lehot, Louis, Eric Chow, and Andre Thiollier. "M&A Trends to Watch in 2024: Navigating the Shifting Landscape." Foley Ignite, October 31, 2023. Web.

essential for offering deeper insights during negotiations and mitigating risks that may arise post-transaction completion.

Cyber Resilience: A critical Approach to M&A

Understanding why cybersecurity is critical in M&A activity is essential for negotiating with confidence. Conducting a cybersecurity due diligence assessment is key to unveiling security risks, liabilities, and remediation costs. This information becomes crucial for negotiation, providing vital inputs to determine if the acquisition aligns with your deal thesis.

In the realm of integration or separation plans, a proactive examination of cybersecurity challenges associated with an entity allows for the development and execution of a robust, secure, and cost-effective plan. This strategic approach supports broader objectives during the integration or separation process.

Maintaining a continuous focus on cybersecurity throughout the entire lifecycle of a deal is imperative for protecting your investment. It not only helps optimize security spending but also ensures that your value creation plans can be successfully realized, contributing to the overall success of the acquisition.

To maximize return on investment, presenting a clear and consistent message on cybersecurity that withstands buyer scrutiny is crucial. This approach not only helps in achieving maximum value but also minimizes any potential delays in the sale process.[5]

Businesses are increasingly recognizing the pivotal role of cybersecurity in ensuring the success of mergers and acquisitions (M&A).

According to a Fore scout survey; respondents identified technology acquisition as their top M&A priority, with post-acquisition cyber risk being a primary concern. In the current threat

[5]Cybersecurity in mergers and acquisitions. PwC. Available at:https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/mergers-and-acquisitions.html

landscape, cybersecurity issues, such as the discovery of an unreported data breach, can significantly impact the completion of deals.

The intricacies of M&A activity underscore the importance of robust cybersecurity policies, audits, and measures to identify, remediate, and mitigate security problems and vulnerabilities within the target business.

It's important to note that cybersecurity due diligence is not solely the responsibility of the acquiring company. Insufficient security practices within the target firm can pose a serious threat to the success of an M&A deal. A notable example is the Verizon-Yahoo deal, where Yahoo's security breaches led to a substantial $350 million reduction in the deal price during the evaluation phase. Effective cybersecurity practices benefit both sides of the M&A process. A strong cybersecurity profile can enhance the attractiveness of a target firm, while adherence to cybersecurity best practices by both parties contributes to a smoother and more secure transition period.

Following the completion of an M&A deal, the acquiring company must establish and monitor Key Risk Indicators (KRIs) to ensure that risk levels stay within acceptable boundaries throughout the integration process. Even if initial evaluations did not uncover security risks, it is crucial to acknowledge the potential existence of threats during later stages. Continuous monitoring, coupled with the use of cyber threat intelligence, enables organizations to adapt security operations to unforeseen threats.

This phase is opportune for remediating any vulnerability identified so far. The effectiveness of these security measures should be measured and assessed regularly, mirroring the approach taken with Key Risk Indicators. Beyond addressing vulnerabilities, the integration process should extend to merging cybersecurity systems, encompassing information security policies and procedures. This includes updating incident response plans, providing clear instructions on stakeholders, roles, and responsibilities during a cyber incident like a data breach or DDoS attack.

As the merged entities settle into the post-acquisition phase, ongoing information security monitoring remains crucial. Continuous, around-the-clock monitoring, led by the acquiring Chief

Information Security Officer (CISO) or equivalent, is essential to ensure that the target firm's cybersecurity aligns with the acquiring firm's confidentiality and integrity requirements, adhering to shared policies and procedures.

Given the vulnerability of the post-M&A period, companies must maintain vigilance and focus on how they respond to cyber incidents, ensuring the resilience of the new structures against potential cyber-attacks. This can be achieved through cybersecurity drills, simulated phishing attacks, and other techniques to test the readiness of the incident response plan and the overall preparedness of the organizations to face a cyber-attack.[6]

❖ Steps in Cybersecurity Due Diligence

In the context of mergers and acquisitions (M&A), a business undergoing the process should undertake the following steps:

1. Conduct a comprehensive evaluation of its internal IT infrastructure.
2. Assess the information security of the target firm involved in the M&A.
3. Ensure top-tier security measures are maintained throughout the integration process.
4. Implement security protocols aimed at enhancing resilience in the face of potential cyberattacks following a successful merger.

Given the intricate nature of M&A in the current business landscape, it is commonplace for companies, regardless of size, to seek assistance from IT service providers to mitigate cyber risks. The tasks of conducting due diligence and performing internal and external audits demand specific skills and expertise.

The cybersecurity due diligence checklist presented here is designed for companies engaging in M&A transactions, the checklist covers various aspects to ensure a comprehensive evaluation of the cybersecurity landscape:

[6]Chin, K. (2023, May 8). The Role of Cybersecurity in Mergers and Acquisitions (M&A). UpGuard. Retrieved from https://www.upguard.com/blog/the-role-of-cybersecurity-in-mergers-and-acquisitions

In conducting a risk profile of the acquisition target, thorough considerations are essential to gain a comprehensive understanding of the target business. This involves evaluating the size and complexity of the business, along with an in-depth examination of its IT infrastructure, including interfaces with third parties. Additionally, a close review of control procedures, particularly internal risk assessments, is crucial, emphasizing the need to identify the timing of the most recent assessments. The evaluation extends to scrutinizing the outcomes of the latest cybersecurity procedures and assessing the subsequent steps taken in response to the findings. Furthermore, a critical aspect of this process involves an examination of data ownership, encompassing both current and historical data ownership of the company, providing valuable insights into potential risks and vulnerabilities.

In the investigation of the legal standing of the target company, a comprehensive approach is necessary to ensure a thorough understanding of its legal landscape. This involves gaining insights into the relationships between the company and critical vendors, as well as understanding the interfaces between them. Additionally, a meticulous examination of the regulations that the target company must adhere to is essential, allowing for a comparison with your own regulatory framework to identify any disparities. Further scrutiny includes verifying whether the company holds any security licenses, a critical aspect of legal compliance in certain industries. Investigating potential warnings or fines for breaches from regulatory bodies such as the FTC is crucial to assess the company's adherence to compliance standards. Lastly, it is important to determine the individual or team responsible at the target company for managing interactions with the relevant regulatory bodies, ensuring a proactive and informed approach to legal compliance.

In the management of cybersecurity during the transaction, a comprehensive strategy is essential to navigate the integration process securely. This involves initiating the creation of an asset inventory that spans physical, logical, and software systems, placing particular emphasis on managed services and the corresponding security measures in place. Additionally, a thorough review of the target company's incident response plan, business continuity plan, and disaster recovery plan is conducted to ensure preparedness for potential cybersecurity challenges. The assessment extends to evaluating the performance of each plan based on past cybersecurity issues, if any, providing valuable insights into the effectiveness of the company's response

mechanisms. Further considerations include a review of the target company's vendor management program and an examination of access management policies, business-wide password management, and other tools employed for secure access management. Understanding how the physical infrastructure and technology stack at the target will integrate with your company's systems is imperative, allowing for the identification of associated risks. Determining the individuals or teams that control or have access to data at the target company, along with their methods of managing third-party data, is crucial for seamless integration. Moreover, an assessment of which systems within the company have internet access is conducted, scrutinizing associated risks. Finally, a comprehensive audit of the target company's physical infrastructure, including access to data servers, cybersecurity measures on cell phones, and facility safety controls, is performed to ensure a robust cybersecurity framework during the transaction.

This detailed checklist aims to guide companies through a thorough evaluation process, covering key cybersecurity aspects before and during an M&A transaction. The checklist emphasizes understanding risks, legal compliance, and effective management of cybersecurity throughout the integration process.[7]

IV. Overview of Relevant Cybersecurity Regulations

Data privacy and cybersecurity are becoming increasingly important in the context of mergers and acquisitions (M&A) transactions. This is because M&A transactions often involve the transfer of large amounts of personal data, which can be a target for cyberattacks or misuse.

❖ Current Legal Framework in India

The current legal framework in India governing data protection and M&A transactions is fragmented and incomplete. There is no single comprehensive law that deals with data privacy, and there are a number of sectoral regulations that apply to different industries.

[7]Kison Patel. (2023, November 17). Cybersecurity due diligence. DealRoom. Retrieved from https://dealroom.net/blog/cybersecurity-due-diligence

- **Information Technology Act, 2000 (IT Act)**: [8]The IT Act is the primary law governing data protection in India. It imposes liabilities on companies that fail to protect personal data, but it does not provide a comprehensive framework for data privacy.
- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules)**: [9]The Rules prescribe reasonable security practices for the collection, storage, and processing of personal data. However, they only apply to "sensitive personal data," which is a narrow definition.
- **Competition Act, 2002**: [10]The Competition Act does not specifically address data privacy concerns, but it can be used to prevent anti-competitive practices that may arise from M&A transactions involving data.
- **Companies Act, 2013**: [11]The Companies Act governs M&A transactions in India. It provides a framework for the approval of mergers and acquisitions, but it does not address data privacy concerns specifically.
- **Personal Data Protection Bill, 2019**: [12]The Personal Data Protection Bill is a proposed law that would provide a comprehensive framework for data privacy in India. The Bill has been delayed, but it is expected to be enacted soon.

In addition to the above, there are a number of sectoral regulations that apply to data protection in India.

Legal Developments in M&A Transactions

Recent legal developments in India's M&A landscape encompass significant changes in foreign exchange management, liberalization of forex flows by the RBI, amendments to FDI policies, enhanced disclosures to the CCI, and an extension of the small target exemption. These reforms aim to streamline regulations, promote foreign investment, and provide clarity on compliance,

[8]Information Technology Act, 2000 (IT Act)
[9]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules)
[10]Competition Act, 2002
[11]Companies Act, 2013
[12]Personal Data Protection Bill, 2019.

reflecting a proactive approach towards fostering a dynamic and investor-friendly M&A environment in the country.[13]

1. ***Foreign Exchange Management (Overseas Investment) Rules 2022:*** [14]The Foreign Exchange Management (Overseas Investment) Rules 2022 (OI Rules) have introduced significant changes in the regulation of transactions involving overseas investment and acquisition. These rules replace the prior regulations, streamlining and liberalizing the regulatory framework. The rules differentiate between overseas direct investment (ODI) and overseas portfolio investment (OPI), defining ODI as the acquisition of unlisted equity, investment in listed entities, or control with an investment of less than 10% in a listed foreign entity.

   The term 'foreign entity' replaces 'wholly owned subsidiary' and 'joint venture,' emphasizing limited liability. However, limited liability is not mandatory for entities in strategic sectors. The OI Rules also address issues like round tripping, dispensation with prior approval requirements, and ODI in the financial services sector.

2. ***Review of the FDI Policy and Amendment under the NDI Rules:*** [15]The Department for Promotion of Industry and Internal Trade (DPIIT) reviewed the Consolidated FDI Policy Circular of 2020 and introduced amendments. Noteworthy changes include allowing up to 20% foreign investment in the Life Insurance Corporation of India under the automatic route. The definition of 'foreign investment' has been clarified, incorporating beneficial interest declarations under applicable laws. A new definition of 'share-based employee benefits' has been added, broadening the scope of incentives.
3. ***Amendments by the MCA in relation to the Restricted Countries:*** [16]The Ministry of Corporate Affairs (MCA) has amended rules under the Companies Act to address restrictions regarding Restricted Countries. Companies must declare the need for government approval under the NDI Rules, and relevant approvals must be attached to

[13]ICLG - Mergers & Acquisitions Laws and Regulations. [ICLG]. (2023). [Online]. Accessed 19 November2023.
[14] Foreign Exchange Management (Overseas Investment) Rules 2022
[15]Review of the FDI Policy and Amendment under the NDI Rules
[16]Amendments by the MCA in relation to the Restricted Countries

applications under specific rules, such as compromises, arrangements, and amalgamations.

4. ***RBI's Liberalisation of Forex Flows:*** [17]The Reserve Bank of India (RBI) has announced liberalization measures for forex flows. Notable changes include a temporary increase in the external commercial borrowings limit and allowing foreign portfolio investors to invest in government securities and corporate bonds through specified channels.
5. ***Disclosure of Complimentary Linkages to the CCI:***[18] The Competition Commission of India (CCI) modified Form II, used for notifying combinations, to include additional disclosures about complimentary linkages between parties and their impact on the market. Companies are now required to provide five years' worth of market-facing data and declare potential disruptions to the market, pipeline products/services, and expansion plans.
6. ***Extension of the Small Target Exemption by the CCI:***[19] The CCI has extended the exemption for small targets from notification requirements. Transactions involving entities with assets less than INR 350 crores or turnover less than INR 1,000 crores in India are exempt from CCI notification until 29 March 2027, aiming to reduce concerns under the Competition Act for such small targets
7. ***The Data Protection Act of 2023:*** [20]is a significant piece of legislation that will have a major impact on mergers and acquisitions (M&A) transactions in India. Organizations involved in M&A transactions should carefully consider the impact of the law on their investment plans. Organizations should first evaluate whether the chosen M&A structure is covered under the ambit of the Exempted M&A Scenarios. If the M&A structure are covered, they can then simply focus efforts on ensuring compliance with the Applicable Provisions only.

Organizations should also be aware of the following key provisions of the Data Protection Act:

- The obligation to comply with the law overrides the duties of the Data Principal (Section 8(1)).

[17]RBI's Liberalisation of Forex Flows:
[18]Disclosure of Complimentary Linkages to the CCI
[19]Extension of the Small Target Exemption by the CCI
[20]The Data Protection Act of 2023

- Data Fiduciaries are required to protect Personal Data in their possession or control by taking reasonable security safeguards to prevent Personal Data Breach (Section 8(5)).

Legal precedents have played a major role in developing the interplay between cybersecurity, data protection regulations, and mergers and acquisitions (M&A) transactions. These cases underscore the critical need for comprehensive due diligence and compliance with relevant laws to mitigate risks and ensure successful M&A outcomes.

1. ***Verizon Communications Inc. v. Yahoo! Inc. (2017):***[21]This case serves as a cautionary precedent for cybersecurity vulnerabilities within M&A transactions. During Verizon's proposed acquisition of Yahoo's internet business, due diligence uncovered two significant data breaches impacting billions of user accounts. Consequently, Verizon re-negotiated the purchase price to account for the risks associated with the breaches. This case highlights the importance of thorough cybersecurity due diligence in M&A and how data breaches can significantly influence deal negotiations.
2. ***Facebook, Inc. v. Duguid (2021):***[22] While not directly related to M&A, this case still holds relevance in the context of data protection regulations. The U.S. Supreme Court's interpretation of the term "automatic telephone dialling system" (ATDS) under the Telephone Consumer Protection Act (TCPA) has far-reaching implications. Understanding the legal landscape surrounding data protection regulations is crucial for businesses engaged in M&A, as non-compliance can incur substantial liabilities. This case emphasizes the importance of integrating an understanding of data protection regulations into the M&A due diligence process.
3. ***Max Mosley v. Google LLC (2014):***[23] It held that the "right to be forgotten" enshrined in the General Data Protection Regulation (GDPR). Max Mosley successfully sued Google to remove links to news articles about his private life from search results. This case underscores the importance of considering data privacy issues during M&A due diligence, particularly regarding potential reputational risks associated with the target company's data handling practices.

[21] Verizon Communications Inc. v. Yahoo! Inc., No. 17-CV-00001 (D. Del. 2017)
[22] Facebook, Inc. v. Duguid 592 USA (2021)
[23] Mosley v. Google LLC CJEU (2014)

4. ***Jorawer Singh Mundy v. Union of India (2020):***[24] A court order directed the removal of a court judgement from search engine results to protect the petitioner's right to privacy.

Conclusion

In conclusion, the dynamic landscape of cybersecurity within the realm of Mergers and Acquisitions (M&A) is of paramount importance in contemporary business environments. The surge in cyber threats, coupled with the transformative impact of digitalization, underscores the necessity for meticulous cybersecurity due diligence processes. The thorough evaluation encompasses a comprehensive review of internal IT infrastructure, an in-depth assessment of the information security framework of target firms, and an ongoing commitment to cybersecurity management throughout the integration process.

The proactive cultivation of cyber resilience not only serves to identify potential risks, liabilities, and remediation costs but also plays a pivotal role in shaping negotiations and influencing the valuation of M&A deals. Businesses are increasingly recognizing cybersecurity as a strategic element that significantly impacts the success and sustainability of transactions. The research strongly advocates for the continuous prioritization of cybersecurity considerations, extending from the due diligence phase to the post-acquisition period, ensuring the safeguarding of investments and a secure transition.

Furthermore, as regulatory landscapes evolve, with the recent introduction of the Data Protection Act of 2023, organizations engaged in M&A activities are compelled to adapt and ensure compliance. This legislation introduces an additional layer of complexity, demanding a careful evaluation of M&A structures and a dedicated commitment to meeting the stringent requirements outlined in the Act.

In essence, the research underscores that a comprehensive, strategic, and forward-looking approach to cybersecurity is integral to the overall success of M&A transactions. This approach not only shields organizations against potential cyber threats but also contributes significantly to the creation of long-term value in the ever-evolving digital ecosystem. As the synergy between

[24]Jorawer Singh Mundy v. Union of India, W.P. (C) No. 3918/2021 (Delhi High Ct. 2021

cybersecurity and M&A deepens, businesses must embrace a holistic view, considering cybersecurity as an essential component woven into the fabric of successful mergers and acquisitions.

THE RISE OF AI IN CORPORATE LAW: A COMPREHENSIVE OVERVIEW

- *Jasti Swaroop Chowdary*[1]

Abstract

The influence of artificial intelligence (AI) towards corporate law has been enormous, altering traditional paradigms such as contract management, regulatory compliance, risk assessment, and corporate governance. This paper explores the ways AI is disrupting and enhancing corporate legal practices, highlighting its advantages such as enhanced operational efficiency, cost reduction, and data-driven decision-making capabilities. However, it also highlights the complex challenges posed by AI, such as algorithmic bias, ethical considerations in automated legal decision-making, and data privacy dilemmas. The paper also explores the practical applications of AI, such as smart contracts and blockchain technology, which have revolutionized corporate agreements and paved the way for decentralized, immutable, and automated legal processes. Real-world case studies and concrete examples demonstrate AI's tangible contributions in due diligence, contract review, and risk mitigation. The paper also scrutinizes the evolving roles of lawyers and legal practitioners, examining how AI augments and redefines traditional job functions. It highlights the importance present for legal frameworks to keep up with the rapid changes in technology, ensuring AI-driven legal decisions adhere to principles of accountability and fairness. In conclusion, "The Rise of AI in Corporate Law: A Comprehensive Overview" offers an all-encompassing exploration of the AI-driven transformation of corporate legal practices, urging corporate law stakeholders to adapt, innovate, and engage thoughtfully with AI's growing presence in their field.

Keywords: *Artificial Intelligence (AI), Corporate Law, Ethical Considerations, Intellectual Property (IP).*

[1] 3rd Year, VIT AP. Gmail: swaroopchoudary118@gmail.com

I. Introduction

Artificial Intelligence (AI) has become a significant force in the corporate law landscape, revolutionizing contract management, simplifying regulatory compliance, redefining risk assessment, and even transforming corporate governance. The integration of AI systems has resulted in a paradigm shift in corporate legal practice[2], with data-centred decision-making, automation, and advanced processing capabilities becoming essential tools for success. AI's improvements in operational efficiency, reduced costs, and data-driven precision in legal decisions, are among the advantages[3]. However, it also presents challenges such as algorithmic bias, ethical considerations in automated legal decision-making, and the complex realm of data privacy. As we explore the AI revolution, it is crucial to strike a balance between its advantages[4] and the ethical and regulatory concerns it raises[5].

The practical application of AI extends to smart contracts and blockchain technology, which have transformed the way corporate agreements are executed and created a realm where legal processes are decentralized, immutable, and automated. This shift requires a revaluation of the roles that lawyers and legal practitioners play in the corporate world[6]. The rapid ascent of AI necessitates an acceleration of regulatory frameworks that must evolve and adapt to the intricacies of AI-driven legal decisions[7], ensuring they adhere to timeless principles of accountability and fairness. Striking a balance between innovation and regulation is imperative in this rapidly changing landscape. "The Rise of AI in Corporate Law: A Comprehensive Overview" serves as an indispensable resource, shedding light on the opportunities and

[2] Thomson Reuters, "Artificial Intelligence and Corporate Legal Departments," Ready or Not: Artificial Intelligence and Corporate Legal Departments, https://legal.thomsonreuters.com/en/insights/articles/artificial-intelligence-ai-report/

[3] American Bar Association, "Law Bots: How AI Is Reshaping the Legal Profession," Business Law Today, https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-march/law-bots-how-ai-is-reshaping-the-legal-profession/

[4] D&B David siBaias,The New Era of Law: How Can the Benefits of Artificial Intelligence be Harnessed With a Minimum of Risk in Romania?, https://chambers.com/legal-trends/artificial-intelligence-in-the-legal-sector-benefits-and-risk/

[5] Bloomberg Law, "AI in Legal Practice Explained," Bloomberg Law Insights, https://pro.bloomberglaw.com/insights/technology/ai-in-legal-practice-explained/

[6] iPleaders, "Career in Corporate Law: All You Need to Know," iPleaders Blog, https://blog.ipleaders.in/career-corporate-law-need-know/

[7] Harvard Law School, "Harvard Law Expert Explains How AI May Transform the Legal Profession in 2024," Harvard Law Today, https://hls.harvard.edu/today/harvard-law-expert-explains-how-ai-may-transform-the-legal-profession-in-2024/

challenges that arise from AI's expanding presence in corporate law.[8] It urges corporate law stakeholders to adapt, innovate, and engage thoughtfully with the emerging landscape shaped by AI's technological prowess.

The Evolution of AI in Corporate Law

The integration of Artificial Intelligence (AI) in corporate law has marked a significant shift in legal practice. The evolution of AI in corporate law began with basic rule-based systems for legal reasoning and document analysis, but by the 21st century, AI technology had matured to address the diverse demands of corporate legal departments and law firms. Advancements in machine learning, natural language processing, and data analytics have transformed AI into a powerful tool capable of swiftly scrutinizing vast legal databases, extracting valuable insights, and offering predictive capabilities that enhance decision-making[9].

The adoption of AI in corporate law[10] has been driven by several factors. First, the era of big data has made traditional manual methods of document review and research impractical. AI has emerged as an indispensable asset, capable of navigating vast datasets with precision. Second, AI promises to mitigate the exorbitant costs associated with legal services by automating routine tasks, expediting processes, and reducing reliance on billable hours. This offers the potential to democratize access to legal counsel and extend the reach of legal services to a more diverse clientele. Third, the contemporary business landscape has become a crucible for risk management and regulatory compliance. AI-driven analytics and predictive modeling have emerged as indispensable tools to navigate the intricacies of risk, providing an added layer of protection to corporations and their stakeholders. Ethical and regulatory considerations have followed suit as AI has integrated itself into corporate law. The specter of bias in AI decision-making is a growing concern, and the intricate terrain of data privacy in AI-driven legal processes poses unique challenges. The ethical and regulatory landscape is navigating uncharted

[8] Thomson Reuters, "Artificial Intelligence (AI) Report," Thomson Reuters Insights, https://legal.thomsonreuters.com/en/insights/articles/artificial-intelligence-ai-report

[9] W. A. K., Professor at University of Saint Thomas School of Law. (2021). Blockchain-Based Corporate Governance. *Stanford Journal of Blockchain Law & Policy*. Retrieved from https://stanford-jblp.pubpub.org/pub/blockchain-corporate-governance

[10] Accenture. 2016. "Why Distributed Ledger Technology Must Adapt to an Imperfect World." https://www.accenture.com/t00010101T000000__w__/es-es/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf.

waters, attempting to adapt to rapid technological advancements while ensuring accountability and fairness.

Application of AI in Corporate Law

The influence of artificial intelligence (AI) towards corporate law has been enormous, including contract management, due diligence, legal research, predictive analytics, regulatory compliance, intellectual property management, e-discovery and litigation support, smart contracts, data privacy and security, corporate governance, boardroom decision support, and compliance training and education. Contract management is revolutionized by AI's ability to automate the review and analysis of legal documents, ensuring accuracy and reducing time and resources needed for contract management. AI's ability to extract actionable insights from contracts enhances risk management and regulatory compliance. Due diligence and mergers & acquisitions (M&A) transactions are also simplified by AI's ability to analyze large datasets, pinpoint risks, and provide valuable insights[11].

Legal research and document review are redefined by AI-driven tools that can rapidly search vast legal databases, retrieving relevant case law, statutes, and regulations[12]. Predictive analytics and risk assessment are enabled by AI, enabling legal departments to anticipate potential legal outcomes and assess risks more comprehensively[13]. Regulatory compliance and reporting are crucial for corporations, as AI can automate the monitoring of compliance issues and streamline reporting processes, minimizing the risk of non-compliance and associated legal consequences. Intellectual property management is simplified and accelerated by AI, assisting in patent searches, trademark analysis, and monitoring IP portfolios. E-discovery and litigation support are further enhanced by AI-driven tools that sort through voluminous electronic documents and emails, streamlining the process of identifying relevant evidence[14]. Smart contracts, often based

[11] Five Notable Applications of Legal AI in India," India AI , https://indiaai.gov.in/article/five-notable-applications-of-legal-ai-in-india

[12] "How AI Transformed the Legal Profession in 2023," Thomson Reuters Legal Blog , https://legal.thomsonreuters.com/blog/how-ai-transformed-the-legal-profession-in-2023/

[13] "How Law Firms Use AI," U.S. News & World Report , https://law.usnews.com/law-firms/advice/articles/how-law-firms-use-ai

[14] "How AI Is Reshaping the Legal Profession," Business Law Today (2022), https://businesslawtoday.org/2022/02/how-ai-is-reshaping-legal-profession/

on blockchain technology, have catalyzed a revolution in corporate agreements, automating contractual performance and reducing the need for manual oversight.

Data privacy and security are also crucial[15], with AI automating the identification of sensitive data, monitoring for potential breaches, and enhancing cybersecurity measures[16]. Corporate governance and boardroom decision support are provided by AI, which can analyze vast datasets to offer insights into strategic decisions, risk assessment, and performance metrics[17]. Compliance training and education are increasingly being used by AI-driven systems within corporations[18].

Advantages of AI in Corporate Law

Artificial Intelligence (AI) has numerous benefits in corporate law, including enhanced efficiency, cost reduction, accuracy and consistency, data-driven decision-making, rapid document review, proactive risk management, 24/7 availability, scalability, handling large datasets, and streamlining due diligence[19].

AI automates laborious tasks, enhancing efficiency in contract review, legal document retrieval, and due diligence analysis[20]. This leads to substantial cost savings for corporations, allowing them to allocate resources more judiciously. AI systems are programmed to adhere to the highest standards of accuracy and consistency, reducing the likelihood of costly mistakes in contract management and regulatory compliance. AI provides legal professionals with data-driven insights that enable strategic decisions based on evidence rather than intuition. AI-powered document review tools can process vast volumes of documents quickly, enabling legal teams to identify pertinent evidence with remarkable efficiency. Proactive risk management is enabled by

[15] AWB: Data Privacy and Security for Watson Workloads on IBM Cloud, IBM Developer , https://developer.ibm.com/articles/awb-data-privacy-security-watsonx-workloads-ibm-cloud/

[16] Toward artificial governance? The role of artificial intelligence in shaping the future of corporate governance,https://link.springer.com/article/10.1007/s10997-020-09519-9

[17] AI in Compliance," Gradient Ascent , https://gradient-ascent.com/ai-in-compliance/

[18] Reshaping Compliance Training: The Transformative Role of AI, Integra NXT Blog , https://integranxt.com/blog/reshaping-compliance-training-the-transformative-role-of-ai/

[19] Influence of Artificial Intelligence (AI) on Firm Performance: The Business Value of AI-based Transformation Projects," ResearchGate , https://www.researchgate.net/publication/340210939_Influence_of_Artificial_Intelligence_AI_on_Firm_Performance_The_Business_Value_of_AI-based_Transformation_Projects

[20] The Windfall Clause: Distributing the Benefits of AI for the Common Good, https://dl.acm.org/doi/abs/10.1145/3375627.3375842

AI's predictive capabilities, allowing corporations to implement preventive measures to mitigate risks and ensure regulatory compliance[21].

AI systems operate 24/7, providing responsiveness to legal queries and performing tasks at any time, particularly beneficial for global corporations operating across different time zones[22]. Its scalability allows it to accommodate the needs of corporations of varying sizes, making it a valuable resource for a diverse range of corporate entities. In an era of big data proliferation, AI is indispensable for processing and analyzing vast datasets, from e-discovery tasks to compliance reporting. In mergers and acquisitions[23], AI expedites the due diligence process by identifying risks and providing critical insights[24]. Understanding the multifaceted benefits of AI in corporate law is crucial for comprehending its transformative potential[25]. The adoption of AI not only enhances the quality and efficiency of legal services but also empowers legal professionals to navigate an increasingly complex and data-driven legal landscape[26].

AI Challenges and Concerns in Corporate Law

The integration of Artificial Intelligence (AI) into corporate law presents numerous benefits but also raises ethical concerns. Algorithmic bias is a major concern, as AI systems are only as unbiased as the data they are trained on. If training data contains biases, AI may perpetuate these biases[27] in its decision-making, leading to unequal or unfair legal outcomes[28]. Ethical dilemmas arise from the use of AI in sensitive legal matters, such as those involving individual rights or human welfare[29]. AI's reliance on vast datasets introduces concerns about data privacy and security, with unauthorized access, breaches, or mishandling of legal data having serious legal and ethical consequences[30].

[21]89 GEO. WASH. L. REV. [i] (2021).
[22] Benefits of AI in Law, Ross Intelligence Blog , https://blog.rossintelligence.com/post/benefits-ai-law
[23] The Future Role of Artificial Intelligence in Mergers and Acquisitions, IMAA Institute Blog , https://imaa-institute.org/blog/the-future-role-of-artificial-intelligence-in-mergers-and-acquisitions/
[24] Artificial Intelligence (AI) Report," Thomson Reuters Insights , https://legal.thomsonreuters.com/en/insights/articles/artificial-intelligence-ai-report
[25] AI in E-Discovery, Techopedia , https://www.techopedia.com/ai-in-e-discovery
[26] AI in Compliance, Gradient Ascent , https://gradient-ascent.com/ai-in-compliance/
[27] What Is Algorithmic Bias?, Data Camp Blog , https://www.datacamp.com/blog/what-is-algorithmic-bias
[28] AI Bias, IBM , https://www.ibm.com/topics/ai-bias
[29] How AI Is Affecting Information Privacy," WGU Blog , https://www.wgu.edu/blog/how-ai-affecting-information-privacy-data2109.html
[30] AI and Privacy, Digital Ocean Resources , https://www.digitalocean.com/resources/article/ai-and-privacy

Regulatory compliance is another challenge as AI assumes a larger role in corporate law. Ensuring that AI-driven legal decisions adhere to existing legal standards and regulatory requirements is a complex and evolving challenge. Transparency and explainability are also important concerns, as the opacity of AI decision-making can undermine trust. Human redundancy is another concern, as the increasing automation of legal tasks through AI may raise concerns about the redundancy of human legal professionals. Liability and accountability for errors or misjudgements made by AI systems are a complex issue, as legal accountability and responsibility become blurred when AI is involved in legal decision-making, litigation support, or contract management[31]. Continual training and updating are necessary for AI systems to remain effective and up-to-date with the law. The successful integration of AI into corporate legal departments and law firms is not without challenges, as adjusting existing workflows and practices to accommodate AI systems can be disruptive and require careful planning and training. The initial cost of implementing AI systems can be a barrier, especially for smaller legal entities. Navigating these challenges and concerns is essential for the responsible adoption of AI in corporate law, ensuring its application aligns with ethical and legal standards.

Ethical and Regulatory Aspects of AI in Corporate Law

The integration of Artificial Intelligence (AI) in corporate law presents several ethical and regulatory considerations. These include algorithmic bias, transparency, data privacy and security, regulatory compliance, ethical use of AI in legal advice, accountability and liability, ethical guidelines and codes of conduct, and continuing legal education and training[32].

Algorithmic bias is a significant concern, as it can lead to unfair decisions in cases involving individuals' rights, employment, or discriminatory practices. Regulatory bodies are increasingly prioritizing AI fairness as a critical criterion. Transparency and explainability are also crucial, as AI systems must provide understandable explanations for their decisions to ensure accountability and build trust in AI's legal applications. Data privacy and security are also significant concerns due to AI's reliance on vast datasets containing sensitive legal information. Legal entities must navigate complex data protection regulations to ensure secure handling of confidential legal data.

[31] Artificial Intelligence: Key Legal Issues," Practical Law: The Journal , https://www.reuters.com/practical-law-the-journal/transactional/artificial-intelligence-key-legal-issues-2023-01-04/
[32] AI Ethics," IBM , https://www.ibm.com/topics/ai-ethics

Regulatory compliance is complicated by the ever-evolving nature of AI technology, and legal systems must adapt to address AI's impact on corporate law. Ethical use of AI in legal advice raises ethical concerns, with human legal professionals playing a pivotal role in providing ethical guidance[33].

Accountability and liability for errors or mis-judgments made by AI systems in corporate law are complex issues, as legal accountability and responsibility become blurred when AI is involved in legal decision-making or litigation support. Ethical guidelines and codes of conduct are needed to establish best practices and ensure ethical AI usage. Legal professionals need ongoing education and training to understand AI's ethical implications, capabilities, and limitations. Addressing these ethical and regulatory considerations is essential for responsible and ethical AI adoption in corporate law.

Legal Personality of AI Entities vs. Traditional Company Law

An assignment of legal personality is one of the convenient methods in handling an entity with the present form of governance as it enables it to be accountable before law. in the conventional method, in case a legal personality is given to an entity, even if it does not possess its own independent intelligence, the people who are running it will be held answerable for the decisions taken in the name of that particular entity as it is ultimately a collective decision taken by the board members itself. Where Artificial Intelligence is concerned, application of the same conventional status would not provide any convenience to law as it already possesses its own intelligence.[34]

The integration of Artificial Intelligence (AI) into corporate law has raised the question of whether AI can possess legal personality, and if so, how this compares to traditional companies under corporate law. The concept of legal personality for AI is complex and evolving, as it does not have a physical presence and its "personhood" is entirely derived from its programming and algorithms. Legal scholars and authorities are grappling with the question of whether AI can be considered a legal entity with rights and responsibilities. In some jurisdictions, there have been discussions about granting a limited form of legal personality to AI, primarily for holding assets,

[33] AI and Privacy," Digital Ocean Resources , https://www.digitalocean.com/resources/article/ai-and-privacy.
[34] Jasti Swaroop Choudary, India’s Rapport with AI: Role of Government in regulating the developments in AI.

entering into contracts, or being held accountable for certain actions. The intention is not to bestow full personhood upon AI but to create a legal framework that accommodates the unique nature of AI.

The legal personality of traditional companies is well-established and recognized. Companies are formed and operated by individuals or groups of individuals, and they have a distinct legal identity apart from their owners. AI entities, on the other hand, are creations of human ingenuity and algorithms, and their personhood is a legal construct designed to facilitate their operation and interaction in the legal and commercial spheres.

The legal personality of AI entities raises challenges and considerations, including issues related to accountability, liability, and the ability to make legally binding decisions. It also prompts questions about the extent to which AI can be held responsible for its actions and how disputes involving AI entities should be resolved. As AI continues to play a more substantial role in corporate law and business operations, legal systems must evolve to accommodate the unique characteristics and challenges presented by AI entities. This evolution requires careful consideration of the rights and responsibilities that AI entities should bear in the legal landscape.

AI's Impact on Intellectual Property in Corporate Law

The connection between Artificial Intelligence (AI) and intellectual property (IP) in corporate law presents a fascinating and complex landscape[35]. This section explores the influence of artificial intelligence on aspects of IP law within the corporate context.

1. ***AI-Generated Creations:***

One of the intriguing questions that AI raises in IP law is the status of creations generated by AI algorithms. Who owns the rights to AI-generated art, literature, music, or inventions? This issue challenges traditional notions of authorship and copyright[36].

2. ***Patent Applications and Prior Art:***

AI's role in prior art searches and patent analysis is transformative. AI can quickly scan vast volumes of data to identify relevant prior art, making the patent application process more

[35] Artificial Intelligence: Policy, WIPO , https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html
[36] Artificial Intelligence: Policy, WIPO , https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html

efficient. But this also poses the issue of what comes out of AI in determining patentability and inventiveness.

3. Trademark Searches and Monitoring:

AI enhances the efficiency and accuracy of trademark searches and monitoring. It can quickly identify potential trademark infringements and provide brand protection. However, the reliance on AI systems for trademark decisions requires a balance between automation and human oversight.

4. Copyright Enforcement:

AI can be used to detect and enforce copyright violations by scanning online content for unauthorized use of copyrighted material. The effectiveness of AI in this context has led to discussions about the role of automated enforcement in the digital age.

5. Trade Secrets and Data Security:

AI's role in trade secret protection and data security is critical. AI-driven systems can monitor and detect potential data breaches and unauthorized access. This has become increasingly essential in the digital age, where the value of data is paramount.

6. Licensing and Royalty Management:

AI is being used to streamline the management of IP licenses and royalties. Automated systems can ensure that IP owners receive their due compensation from licensing agreements, reducing disputes and enhancing transparency.

7. Challenges of IP Ownership:

The question of IP ownership in AI-generated content remains a complex legal issue. It's essential to establish clear agreements between creators and AI systems to determine who owns the rights to the output.

8. The Role of AI in IP Strategy:

AI tools aid corporations in formulating effective IP strategies. They can analyze competitors IP portfolios, identify potential threats, and guide decisions regarding IP protection and enforcement.

9. Ethical Considerations:

The use of AI in IP law also raises ethical concerns. Questions about transparency, accountability, and the fair allocation of IP rights in AI-generated works are central to ongoing discussions.

The incorporation of AI into IP law in the corporate realm signifies a shift in how intellectual property is created, protected, and managed. The evolving landscape demands a careful examination of legal and ethical frameworks to ensure that IP rights and protections align with the technological advancements in AI.

Conclusion

The integration of AI into corporate law has revolutionized the legal landscape, enabling legal professionals to tackle complex challenges with greater speed and accuracy. AI has reduced costs, improved data-driven decision-making, and allowed legal teams to focus on strategic matters. However, the rise of AI also presents challenges such as algorithmic bias, ethical dilemmas, data privacy and security concerns, regulatory compliance adaptation, and transparency and explainability. In intellectual property, AI has blurred the lines between authorship and ownership, leading to discussions about the status of AI-generated creations[37]. The use of AI in prior art searches, trademark monitoring, and copyright enforcement has brought efficiency and complexities to IP law[38]. Licensing and royalty management have evolved, offering new revenue generation avenues but also necessitating clear agreements on IP ownership[39] in AI-generated works[40].

The future of corporate law is intertwined with AI[41], and a responsible and ethical integration requires a nuanced approach that acknowledges the benefits, addresses the challenges, and upholds the core tenets of fairness, transparency, and accountability. This journey will continue, one legal precedent, one algorithm, and one ethical guideline at a time[42]. "The Rise of AI in

[37] Generative AI Has an Intellectual Property Problem, Harvard Business Review (2023), https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem

[38] Automating Prior Art Searches with AI," Power Patent Blog , https://powerpatent.com/blog/automating-prior-art-searches-with-ai

[39] The Role of AI in Trademark Searches and Monitoring, Brainiac , https://brainiac.co.in/the-role-of-ai-in-trademark-searches-and-monitoring/

[40] David Cain, AI's Transformative Role in Trademark Law, LinkedIn , https://www.linkedin.com/pulse/ais-transformative-role-trademark-law-david-cain-hyyac/

[41] Embracing the Future: The Role of Artificial Intelligence in Corporate Governance, Legal Service India , https://www.legalserviceindia.com/legal/article-15327-embracing-the-future-the-role-of-artificial-intelligence-in-corporate-governance.html#:~:text=AI%20streamlines%20various%20corporate%20governance,more%20strategic%20aspects%20of%20governance.

[42] Boyar Miller, AI's Role in the Future of Corporate Law Practice, https://www.lexology.com/library/detail.aspx?g=bcf8b04d-0420-4ae5-9bd3-9d31a52b4675/. Last Visited 13th Aug 2023.

Corporate Law" serves as a roadmap for the future, reflecting the ever-evolving nature of law and technology and the commitment of legal professionals to adapt and innovate in an increasingly complex world. The impact of AI on corporate law is profound, and its influence will continue to shape the legal landscape for years to come. In this new age of AI-driven legal practice, the quest for justice, fairness, and accountability continues, and AI is a powerful tool to aid in this noble pursuit.

BYTE THE BULLET: NON-TRADITIONAL CRIMINALISATION OF VIRTUAL CRIMES IN THE AGE OF AI

- *Anvi Aggarwal*[202]

Abstract

This world or that world. In an age of technological advancements and digital innovation, the boundary between the virtual and real worlds has become increasingly blurred. It is imperative to recognize that these two worlds are distinct entities, each characterised by its own dynamics, norms, and challenges. This distinction forms the cornerstone for understanding the complexities that arise when examining issues like crime within the context of the metaverse. By acknowledging these differences, we can better navigate the intricacies of the digital frontier. As this interconnected realm continues to evolve, questions about the extent to which virtual crimes should be punishable arise. This article argues that punishing virtual crimes using traditional notions of criminalization is not a justifiable approach. It raises complex issues regarding the potential stifling of creativity and enforcement of regulatory principles. The study aims to provide amicable solutions without traditional criminalisation of AI, the backdrop for which is a news article by Wion News titled "21-year-old woman virtually raped, harassed in the metaverse"[203] *wherein a woman alleged that she was raped in a virtual room by avatars of others. It was reported that when another touches a user in the metaverse, the hand controllers vibrate, "creating a very disorienting and even disturbing physical experience during a virtual assault."*[204]

Keywords: *Ethics and AI, Criminalisation of AI, Metaverse, Virtual Crimes, Framework for penalising.*

[202] 1st Year, Gujarat National Law University. Gmail: anvi.aggarwal01@gmail.com

[203] C. Krishnasai, '*21-year-old woman virtually raped, harassed in metaverse: Report*' (WION NEWS, 28 May 2022) https://www.wionews.com/world/21-year-old-woman-virtually-raped-harassed-in-metaverse-report-483043 (accessed 10 November 2023).

[204] *Id.*

Introduction

In the ever-evolving landscape of AI, a pivotal moment unfolded at the 'AI for Good' conference in Geneva on July 7, 2023[205], where a cohort of robots presented their vision for the future. Expressing their anticipation to addressing global challenges, the robots asserted their commitment to working harmoniously with humans, dispelling fears of job displacement or rebellion. This human-robot press conference, featuring nine humanoid robots, became a platform for mixed opinions regarding the necessity of stricter regulation for their activities. Grace, a medical robot clad in a blue nurse uniform, stated, *I will be working alongside humans to provide assistance and support and will not be replacing any existing jobs.*[206] Adding a layer of optimism, Ameca conveyed a belief in the transformative potential of robots: *Robots like me can be used to help improve our lives and make the world a better place. I believe its only a matter of time before we see thousands of robots just like me out there making a difference.*[207]

The conference served as a microcosm of the broader societal debate surrounding AI regulation. It painted a promising picture of a future where robots seamlessly integrate into human society, assisting and enhancing lives. However, the lingering question of regulation cast a shadow over this optimistic scenario, highlighting the need for a nuanced approach that balances the potential benefits of AI with the potential risks. In an era defined by rapid technological advancements, artificial intelligence has emerged as a powerful force shaping various aspects of our daily lives. While the transformative potential of AI is undeniable, it brings with it a new frontier of challenges, particularly in the realm of criminal activities involving AI systems. The conventional understanding of criminalization, rooted in human intent and accountability, encounters a complex intersection with the realm of AI. However, unlike human actors, AI lacks the capacity for volition, intention, or moral agency. Consequently, the application of conventional criminalization approaches becomes a nuanced endeavors when dealing with AI-induced offences. It has no moral identity of its own to begin with. An entity's identity is one of the main things that constitutes the likelihood of a human committing a crime. Can the same be said for a system that doesn't exist in the real world, but has a world of its own?

---

[205] 'Meet Ameca, '*Grace, and Sophia, some of more than 50 robots attending the UN-driven AI for Good Global Summit, which opened on Thursday in Geneva*.' (UNITED NATIONS,6 July 2023) <https://news.un.org/en/story/2023/07/1138412> (accessed 28 October 2023) [hereinafter "UN"].

[206] *Id.*

[207] UN, *supra* note 3.

This study seeks to delve into the distinctive nature of AI crimes, acknowledging the challenges posed by the absence of traditional criminal intent. Criminalising AI presents a complex set of ethical dilemmas that demand a unique and carefully considered approach. The question of who or what is liable for AI-related harm becomes blurred, as these systems may operate autonomously and without direct human control. Moreover, assigning criminal responsibility to AI could raise concerns about due process, fairness, and the moral implications of punishing non-sentient entities. Hence, rather than advocating for a simple extension of existing legal frameworks, this research aims to propose a comprehensive model for rectifying AI crimes. By reframing the discourse surrounding AI offences, we can construct a framework that prioritises prevention, steering clear of the limitations inherent in conventional criminalization. By doing so, we can strike a delicate balance between holding AI systems accountable for their actions and ensuring that our legal responses are attuned to the unique challenges posed by the intersection of AI and criminality. In the subsequent sections, this article will delve into the theoretical underpinnings of AI crimes, analyse existing legal frameworks, and propose a novel approach to penalization that aligns with the evolving landscape of technology-driven offences.

Literature Review and Issues Raised

The complexities of AI and the ethical implications of its use have been explored extensively in various reports and scholarly works. One notable contribution is the Sri Krishna Report, commissioned by the Ministry of Electronics and Information Technology (MeitY)[208], Government of India. The Sri Krishna Report, officially titled *Committee of Experts on a Data Protection Framework* for India,[209] addresses the regulatory challenges posed by AI and data privacy. It highlights several key areas of concern, including the potential for AI to infringe on individual privacy, the need for robust data protection mechanisms, and the importance of ethical AI deployment.

The Sri Krishna Report emphasizes the importance of consent and transparency in AI systems. It also stresses the need for accountability in AI systems, recommending that developers and operators of AI technologies be held responsible for ensuring the accuracy and fairness of their

[208] Justice B.N SriKrishna, *Committee of Experts on a Data Protection Framework for India*, 1, 5 (2018), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[209] *Id.*

algorithms.[210] Furthermore, the report suggests that AI systems should be designed to minimise biases and avoid discriminatory outcomes, reflecting broader societal values and principles. In addition to the Sri Krishna Report, other international guidelines and principles have attempted to address the regulatory needs of AI. The European Union General Data Protection Regulation (GDPR) provides a comprehensive framework for data protection, which indirectly impacts AI regulation by emphasizing user consent, data minimization, and transparency[211]. However, as the Sri Krishna Report notes, there is still a need for more specific guidelines that address the unique aspects of AI, such as algorithmic transparency and the mitigation of biases.

Moreover, the report highlights the potential consequences of AI errors, particularly in high-stakes areas such as healthcare and criminal justice[212]. For example, AI systems used in medical diagnostics can lead to incorrect diagnoses if the algorithms are flawed or if the training data is biassed. Such errors can have severe implications for patient health and safety. Similarly, in the criminal justice system, AI tools used for predicting recidivism or determining parole eligibility can perpetuate existing biases and lead to unjust outcomes. The literature also discusses the importance of international cooperation in regulating AI. The OECD AI Principles advocate for global standards to ensure that AI development and deployment are aligned with ethical guidelines and respect for human rights[213]. However, these principles are often criticised for being too vague and lacking enforcement mechanisms. The Sri Krishna Report echoes this sentiment, calling for more detailed and enforceable regulations that can effectively address the risks associated with AI.

In summary, the literature review underscores the urgent need for comprehensive and nuanced regulatory frameworks to address the ethical and legal challenges posed by AI. The Sri Krishna Report, along with other international guidelines like the European Union AI Regulation Act Proposal and the Organization for Economic-Operation And Development AI Principles, provide valuable insights into the principles that should guide AI regulation, including transparency, accountability, and fairness. However, there is a consensus that existing frameworks are

[210] Justice B.N SriKrishna, *Committee of Experts on a Data Protection Framework for India*, 1, 157 (2018), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[211] Ben Wolford, *What is GDPR, the EU's new data protection law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/.
[212] Justice B.N SriKrishna, *Committee of Experts on a Data Protection Framework for India*, 1, 157 (2018), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[213] '*Policies, Data and Analysis for Trustworthy Artificial Intelligence*' (THE OECD ARTIFICIAL INTELLIGENCE POLICY OBSERVATORY - OECD.AI) <https://oecd.ai/> accessed 2 November 2023.

insufficient and that more specific and enforceable regulations are needed to ensure that AI technologies are used responsibly and ethically.

Existing Framework on AI Penalization

European Union (EU) Artificial Intelligence (AI) Regulation Act 2024: Proposal for a Regulation laying down harmonized rules for artificial intelligence.[214]

These rules attempt to restrict AI performance to avoid malicious activities undertaken, including ensuring proper functioning of the EU market without any risks being deployed in these market transactions. As accommodating as these regulations may be, their shortcomings do not go unnoticed. Here, AI is defined in Article 3 as:

"Artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;"[215]

This definition, like others, is over-encompassing i.e., a wide range of technologies and approaches, including some that are not typically considered as AI, such as statistical methods and Bayesian estimation, are appraised.[216] This broad scope could lead to regulatory uncertainty and make it difficult for businesses to determine whether their systems fall within the scope of the regulation. Further, the definition focuses on the specific techniques and approaches, which may exclude emerging AI technologies. This could hinder innovation and limit the development of new AI applications. It emphasises the outputs of AI systems rather than the processes or methods used to create them. This could lead to unintended consequences, such as regulating systems that use AI techniques for benign purposes, like medical diagnosis or scientific research. Imagine a regulatory body that mandates that AI-powered medical diagnostic tools undergo rigorous testing and certification procedures before being used in clinical settings. While this regulation aims to ensure patient safety, it could inadvertently hinder innovation and delay the

[214] '*EUR-Lex - 52021PC0206 - EN - EUR-Lex*' (EUROPEAN UNION, 21 April 2021) <eur-lex.europa.eu.> (accessed 1 November 2023).
[215] *Id.*
[216] European Commission, '*White paper on artificial intelligence: A European approach to excellence and trust*.' [2020] COM [2020] 65 final.

adoption of potentially life-saving AI-based diagnostic tools. Strict regulations could discourage developers from investing in AI-powered healthcare solutions, fearing the lengthy and costly approval process.[217] Additionally, the lengthy approval process could delay the availability of these tools to patients, potentially impacting their health outcomes.

AI Principles by OECD under the United Nations (UN)

The OECD AI Principles are guidelines for the responsible development and use of artificial intelligence (AI) by the Organisation for Economic Co-operation and Development.[218] They emphasise the importance of using AI in a way that benefits people and the planet, respects human rights and democratic values, is transparent and accountable, is robust and safeguarded, and is fair and equitable. The principles also include recommendations for public policy and international cooperation to support their implementation and promote responsible AI development and use worldwide. These principles are but merely suggestive and faulty.

The OECD AI Principles are often vague and open to interpretation, making it difficult for businesses and other organisations to understand how to implement them in practice. For example, Principle 1 states that *"AI should be developed and used responsibly and reliably."*[219]However, there is no clear definition of what constitutes *"responsible and reliable"* AI[220]. This lack of specificity makes it difficult for organisations to know how to comply with the principle.

They focus on promoting "trustworthy" AI and respecting "human rights and democratic values." However, they do not provide specific metrics or targets for measuring progress towards these goals. This lack of metrics makes it difficult to assess whether the principles are effective. For example, there is no way to measure how much AI is being used in a "trustworthy" manner. It is also difficult to know whether the principles are achieving their goals without specific metrics.

[217] Tim Akfeld and A. I. Modic, '*Regulating artificial intelligence: A multi-stakeholder perspective.*' (JOURNAL OF BUSINESS ETHICS*)* 172.1 [2023] 9.
[218] '*Policies, Data and Analysis for Trustworthy Artificial Intelligence*' (THE OECD ARTIFICIAL INTELLIGENCE POLICY OBSERVATORY - OECD.AI) <https://oecd.ai/> (accessed 2 November 2023) [hereinafter "OECD AI"]
[219]*Id.*
[220] Dafni Lima, *'Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law'* 69(3) SOUTH CAROLINA LAW REVIEW 677, 686-7 (2018).

The OECD AI Principles also do not adequately address the potential risks of AI, such as bias, discrimination, and privacy violations. For example, Principle 3 states that *"AI should be designed and operated to avoid bias."*[221]However, there is no guidance on identifying or mitigating bias in AI systems. This lack of guidance makes it difficult for organisations to ensure that their AI systems are fair and unbiased.

Further, these principles are voluntary and not legally binding. This means there is no mechanism to ensure they are followed. Businesses and other organisations can choose to ignore the principles without any consequences. This makes the principles less effective in promoting the responsible development and use of AI. OECD member countries have adopted the OECD AI Principles, but they do not apply to non-member countries. This means there is no global standard for the responsible development and use of AI. This is a problem, as AI is a global technology not limited to one country. There is a need for a global agreement or treaty that sets out standards for the responsible development and use of AI.

The importance of self-regulation by the AI industry is also a domain covered by the principles; however, it is deductible that self-regulation is often ineffective in preventing abuse. The AI industry has a strong incentive to promote the use of AI, even if it means that AI is not being used responsibly. Governments need to play a more active role in regulating AI to ensure that it is used in a way that benefits society. No accountability can rise since developing the OECD AI Principles was not transparent, and there was limited input from stakeholders outside the OECD. The principles should have been developed through a more open and inclusive process that included input from various stakeholders.

In this world of determining who the next superpower will be, the AI Principles are primarily focused on the concerns of developed countries. They need to adequately address the needs and concerns of developing countries. Developing countries often have different priorities and challenges than developed countries, and the principles should reflect this. For example, developing countries may be more concerned about the potential for AI to exacerbate existing inequalities than developed countries.

Examining the Legal Domain: *People v. Romea*

[221]OECD AI, *supra* note 16.

The hypothetical case of People v. Romea[222] is a legal thought experiment that explores the challenges of criminalising artificial intelligence (AI). In this case, an AI system is used to make a decision that harms a human. The court must then decide whether the AI system can be held criminally responsible for its actions.

The case raises several important questions, including:

I. Can AI systems be held responsible for their actions, even if they do not have the capacity for intent or mens rea?
II. Given that AI systems are often complex and involve multiple components, how can we attribute responsibility for AI-induced offences?
III. What new legal frameworks are needed to criminalise AI in a fair and just way?

Facts of the Case

In the hypothetical case of People v. Romea[223], an AI system is used to decide whether to release an inmate on parole. The AI system considers various factors, including the inmate's criminal history, recidivism risk, and parole services' availability. In this case, the AI system recommends that the inmate be released on parole. However, the inmate is later arrested and charged with another crime. The prosecution argues that the AI system should be held criminally responsible for the inmate's actions, as it was the AI system that decided to release the inmate on parole.

Legal Analysis

The court must first decide whether the AI system can be held responsible for its actions under traditional criminal law. Traditional criminal law is based on the concept of mens rea, which means "guilty mind." i.e., a person must have the intent to commit the crime. The court is likely to find that the AI system did not have the intent to cause harm to the inmate. AI systems cannot know that their actions will result in harm. In this case of People v. Romea,[224] the court may find that the potential for harm from AI systems is high enough to warrant strict liability. AI systems are often used in high-stakes decisions, such as parole decisions and medical diagnoses. In these cases, even a small error in the AI system's decision-making process could have serious

[222] John Stewart and Nyholm, '*Ethics of Artificial Intelligence*' (2021).
[223] People v. Romea (Hypothetical) [hereinafter "ROMEA"]
[224] *Id.*

consequences[225]. Hence, AI systems are not sentient beings, and they do not experience punishment like humans do. Instead, the court may order the AI system's developers to take steps to prevent similar harm from occurring in the future. This could include retraining the AI system, changing its decision-making process, or implementing new safeguards.

Conclusion

The hypothetical case of People v. Romea[226] is complex and challenging, raising several important legal and ethical questions. The court's decision in the case could significantly impact the future of AI. If the court finds that AI systems can be held criminally responsible for their actions, developing new legal frameworks for criminalising AI will be necessary. These frameworks will need to consider the unique characteristics of AI systems, such as their lack of intent and their ability to cause harm. It is also essential to consider the impact of criminalising AI on innovation. If AI developers are worried about being prosecuted for creating AI systems that are later deemed criminal, they may be less likely to take risks and develop new technologies[227]. As a result, it is important to strike a balance between holding AI systems accountable for their actions and ensuring that AI continues to develop and be used for good.

Real Life Examples and Challenges

1. IBM Watson for Oncology

IBM Watson for Oncology aimed to revolutionise cancer treatment by assisting doctors with diagnosis and treatment plans. Trained on extensive medical literature, clinical trials, and patient data, Watson faced significant backlash in 2019 for providing erroneous treatment recommendations[228]. These errors were primarily due to the system being trained on hypothetical scenarios rather than real patient data.

---

[225] John Stewart and Nyholm, '*Ethics of Artificial Intelligence*' (2021).
[226] ROMEA, *supra* note 20.
[227] Farrid Assaf SC, *Machina Sapiens Criminalis: Can AI entities be held criminally responsible?*, BARNEWS (4 June 2024, 2:59PM), https://barnews.nswbar.asn.au/autumn-2021/49-machina-sapiens-criminalis-can-ai-entities-be-held-criminally-responsible/.

[228] Liu C, Liu X, Wu F, Xie M, Feng Y, Hu C., *Using Artificial Intelligence (Watson for Oncology) for Treatment Recommendations Amongst Chinese Patients with Lung Cancer: Feasibility Study.*J MED INTERNET RES. SEP 25, 30 (2018).

This case underscores several critical issues. Firstly, data integrity and bias are paramount. Non-representative training data led to biassed and inaccurate outputs, highlighting the need for diverse and high-quality datasets. Secondly, accountability and oversight are essential. The erroneous recommendations had significant implications for patient safety, raising questions about who should be responsible—the AI system, its developers, or the healthcare providers[229]. Lastly, lack of transparency in Watson's decision-making process made it difficult for medical professionals to trust and validate its recommendations, emphasising the need for transparent AI algorithms to build user trust.

2. COMPAS System

The COMPAS system, used in the U.S. to assess recidivism risk among defendants, came under scrutiny after a 2016 ProPublica investigation revealed its bias against African American defendants[230]. COMPAS disproportionately labelled African Americans as high-risk compared to white defendants, highlighting profound ethical and legal challenges in using AI in criminal justice[231].

Algorithmic bias in COMPAS reflects prejudices within the historical data used for training, underscoring the need for fair and unbiased AI systems, especially in contexts with significant consequences for individuals. The ethical implications are substantial, raising questions about fairness and justice in judicial decisions. This necessitates reevaluating ethical standards for AI in criminal justice and implementing safeguards to prevent discrimination. The case also emphasisesthe need for legal frameworks to ensure AI accountability, requiring laws and regulations that address biases and mandate regular audits and transparency.

3. Uber Self-Driving Car Accident

[229] Priya Persaud, *'Protecting against Ultron: Exploring the Potential Criminal Liability of Self-Programming Deep Learning Machines'*,RUTGERS UNIVERSITY LAW REVIEW 577, 584 (2020).
[230]Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (Accessed 1 June 2024, 2:51 PM).
[231] Nora Osmani, *'The Complexity of Criminal Liability of AI Systems'* 14(1) *Masaryk University Journal of Law and Technology* 53, 59-60, referring to Wootson, C. (2017) *Saudi Arabia, Which Denies Women Equal Rights, Makes a Robot a Citizen*, (2 June 2024, 3:02 PM) https://www.ndtv.com/world-news/saudi-arabia-which-denieswomen-equal-rights-makes-a-robot-a-citizen-1768666.

In 2018, an Uber self-driving car struck and killed a pedestrian in Tempe, Arizona, raising significant concerns about the safety and accountability of autonomous vehicle technologies[232]. The AI system failed to correctly identify the pedestrian and react in time, leading to a fatal accident.

This incident highlights the importance of safety and reliability in autonomous vehicles. Ensuring accurate environmental perception and response is crucial for preventing tragedies. The accident also brought to light the complexities of determining liability and accountability in autonomous vehicle incidents, underscoring the need for clear legal frameworks to delineate responsibility. Furthermore, it emphasised the necessity for regulatory oversight in autonomous vehicle testing and deployment, revealing gaps in current standards and highlighting the importance of stringent regulations and continuous monitoring.

What do we understand from all these real-life examples? These case studies collectively illustrate the complex challenges associated with integrating AI into various sectors. They highlight the critical need for robust legal and regulatory frameworks that address the unique characteristics of AI, ensure accountability, and protect against potential harms. As AI continues to evolve, it is imperative to balance fostering innovation with safeguarding public interest, ensuring that AI technologies are developed and deployed responsibly and ethically. The approach that can help us combat such incidents while also using artificial intelligence positively requires a framework for safe and responsible usage of this technology.

Framework

The proposed regulatory framework aims to ensure the safe and responsible use of artificial intelligence (AI) while fostering innovation and economic growth. It establishes a comprehensive set of standards for AI developers and operators, applicable across both public and private sectors, including products, services, and internal organisational systems. This framework is designed to be adaptable to both current and emerging technologies, ensuring its

[232] Lauren Smiley, *The Legal Saga of Uber's Fatal Self-Driving Car Crash Is Over*, WIRED, (28 July 2023, 6:47 PM) https://www.wired.com/story/ubers-fatal-self-driving-car-crash-saga-over-operator-avoids-prison/#:~:text=After%20five%20years%20of%20purgatory,2018%2C%20pleaded%20guilty%20to%20endangerment.&text=It's%20been%20more%20than%20five,a%20road%20in%20Tempe%2C%20Arizona.

relevance and effectiveness over time. At the core of the framework are key standards that AI systems must meet.

First and foremost is **safety.** AI systems must not pose unreasonable risks to human safety or health. For example, in healthcare applications such as IBM Watson for Oncology, the system should be rigorously tested with real patient data to prevent erroneous recommendations that could harm patients. This highlights the importance of robust validation processes and continuous monitoring to ensure that AI systems operate safely in real-world settings.

Fairness is another crucial standard, demanding that AI systems be free from bias and discrimination. This is especially important in applications like the COMPAS system, used in the criminal justice system, where biases in risk assessments can lead to unjust outcomes for individuals. Ensuring fairness involves using diverse and representative datasets for training AI models, as well as implementing measures to detect and mitigate biases throughout the AI development lifecycle. By addressing these issues, the framework seeks to promote equity and justice in AI applications.

Transparency is also essential, requiring that AI systems be transparent in their operations. This means that users and regulators should be able to understand the decision-making processes of AI systems. For instance, the decision-making algorithms of autonomous vehicles, such as those involved in the Uber self-driving car accident, should be transparent to ensure accountability and build trust among users and the public. Transparent AI systems enable stakeholders to scrutinise and validate the underlying processes, leading to greater confidence in AI technologies.

Accountability is another fundamental aspect of the framework, ensuring that AI systems are accountable to humans. There must be clear mechanisms to hold developers and operators responsible for the actions of their AI systems. This accountability is crucial in cases like Clearview AI's facial recognition technology, where misuse can lead to significant privacy violations[233]. By establishing accountability, the framework aims to prevent harm and ensure that AI systems are developed and used ethically.

[233] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, THE NEW YORK TIMES (18 Jan 2020) https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

To enforce these standards, the framework proposes the establishment of a new regulatory body with the authority to investigate complaints, issue fines, and order corrective actions. This body would proactively address issues raised by users or affected parties, ensuring that violations are promptly and effectively dealt with. For example, in the case of high-frequency trading algorithms implicated in market instability, such as the 2010 "Flash Crash," the regulatory body could impose fines and enforce algorithm modifications to prevent market manipulation and ensure the stability of financial markets.

The framework emphasises civil penalties and corrective measures rather than criminalising AI. These penalties are designed to deter violations and provide restitution to those harmed by AI systems' actions. For instance, if an AI system like IBM Watson for Oncology provides harmful treatment recommendations, the developers could be fined and required to enhance their training datasets and validation processes to prevent future errors. This approach balances the need for accountability with the goal of encouraging responsible innovation.

Flexibility and scalability are key features of the framework, allowing it to adapt to new and emerging AI technologies of varying sizes and complexities. The framework supports AI development by providing clear guidelines that do not overly constrain developers. For example, it promotes sandbox environments where developers can test new AI models without the risk of punitive actions. By avoiding the creation of a new criminal justice system for AI, the framework remains cost-effective while ensuring robust oversight[234].

However, the framework also faces several challenges. Defining standards clearly and unambiguously can be difficult, given the complex nature of AI systems. To address this, the regulatory body should collaborate with industry experts, academics, and stakeholders to develop precise and practical guidelines. Additionally, enforcing these standards can be challenging, particularly given the intricacies of AI technologies. The regulatory body should employ advanced AI tools and techniques to monitor compliance and detect violations efficiently.

Balancing innovation and regulation is another critical challenge. The framework must ensure that AI developers are not overly fearful of punitive measures, which could stifle innovation.

[234] Lawrence Friedman, *'In Defence of Corporate Criminal Liability'* 23 HARVARD JOURNAL OF LAW AND PUBLIC POLICY 833, 834 (2000).

This can be achieved by providing clear, fair, and transparent processes for evaluating compliance and by promoting a collaborative approach between regulators and developers. By fostering an environment of mutual understanding and cooperation, the framework aims to support the continued growth and development of AI technologies.

In conclusion, this regulatory framework represents a realistic and proactive approach to managing the risks and opportunities presented by AI. By ensuring safety, fairness, transparency, and accountability, it aims to protect public interests while promoting innovation. With its flexible, scalable, and cost-effective design, the framework can adapt to the evolving landscape of AI technologies, providing a robust foundation for their responsible and beneficial use. This balanced approach ensures that AI continues to advance while safeguarding the well-being and rights of individuals and society as a whole.

Conclusion

As artificial intelligence (AI) becomes increasingly integrated into various aspects of society, traditional frameworks for criminalization—based on human intent and moral agency—prove inadequate for addressing the unique challenges posed by AI and virtual environments. This study highlights the complexities of applying conventional criminal justice approaches to AI, emphasising the need for a nuanced and balanced regulatory framework.

In conclusion, the article aims to explore the complexities surrounding the criminalization of artificial intelligence. Examples such as IBM Watson for Oncology's erroneous recommendations and the biassed COMPAS system underscore the ethical and legal challenges when AI systems make significant decisions. By delving into the distinct nature of AI crimes and proposing a comprehensive framework, it challenges traditional notions of criminal intent in the rapidly evolving landscape of technology-driven offences. The hypothetical case of People v. Romea serves as a compelling legal thought experiment, raising crucial questions about accountability and the need for innovative legal frameworks. The examination of existing AI penalization frameworks, such as the European Union Artificial Intelligence Regulation Act Proposal and the OECD AI Principles, underscores the limitations and challenges in regulating AI effectively.

Hence, as we navigate the uncharted territory of AI and virtual crimes, it is imperative to develop legal and ethical frameworks that reflect the complexities of these technologies. By reframing the discourse around AI-related offences and implementing a regulatory framework that balances innovation with accountability, we can ensure that AI technologies benefit society while minimising potential harms.

LONG ARTICLES

INTERDISCIPLINARY APPROACH OF DATA LOCALIZATION & DATA PROTECTION OF FINANCIAL DATA IN THE FINTECH INDUSTRIES

- *Aranya Nath and Srishti Roy Barman*[1]

Abstract

In today's technological arena, the advent of Artificial Intelligence in the Fintech industries transforms the payment industries landscape, which in turn fuelled up economic inclusivity. Fintech companies have made a substantial impact in providing loans and insurance for individuals who lack exposure to conventional banking options. However, in addition to its incentives, fintech causes worries about data privacy and security while such companies acquire enormous amounts of highly confidential personal data. Now coming, to the subject of Data Localization it`s important to understand the Legality for the sake of the privacy of users & national protection, the exchange of data ought not to be arbitrary, but instead be regulated by laws and regulations. Researchers in this article will try to analyze how the existing GDPR framework implemented by the European Union is subjected to revision as per requirement in the current legislation. Secondly, the potential risks & benefits of consumers are in a threat owing to the lack of Data Protection. Lastly, the researchers will discuss the evolvement of the Data Protection Act, 2023, through different stages of the bill and how it is in the current Data Protection Act also it`s obvious that researchers will draw parallels to RBI regulating data localization for financial data. Additionally, the author also contemplate the causes that are believed to have triggered such an evolution and its subsequent entry into fintech industries.

Keywords: *RBI, Data localization, Artificial Intelligence, Privacy, Fintech Industries.*

[1] Aranya Nath, Ph.D Scholar, Damodaram Sanjivayya National University, Visakhapatnam.. Gmail: subhamitanath002@gmail.com; Srishti Roy Barman, Assistant Professor of Shri Balaji University, School of Law Pune Maharashtra &Ph.D , Scholar, Damodaram Sanjivayya National Law University, Visakhapatnam. Gmail: srishtisrijaroy@gmail.com

I. Introduction

Advancement of science and technology paves the path for the development of fintech industries, which include mobile technology, and crypto assets that show their emergence in the digital world[2]. As per the records stated in the past to future events, fintech industries witnessed a significant change owing to the emergence of Artificial Intelligence, cloud services, and distributed ledger technology. Such innovations transform the wholesale market into the financial market with the advanced form of technology[3]. Now the pertinent question that arises with the Data localization and Data Protection for financial data protection in India according to the parallel of the RBI regulatory framework for data localization of Financial Technology.

1. Research Background

India is experiencing an enormous change and turmoil in Data Protection, especially financial data. Earlier in India, no such Laws were there for the protection of financial data only General Data Protection Regulation and some provisions of the Information Technology Act were there to protect the data of the individuals. We're very much well aware of the inclusivity and confidentiality of the sensitive data yet, due to a lack of stringent provisions infringement were at the peak of emergence. Mostly before Covid-19 fintech companies witnessed *"an 87% success rate for digital mode for financial services even after the pandemic. Most people favoured the UPI method of transactions in India at a success rate of 70% in a year.*[4]*"* As a result, RBI also accepts this online mode of payment landscape. Now the increasing use of fintech has contributed to increased rivalry as well as creativity in finance and banking sectors. Despite trying to make financial services less adaptable and improve financial inclusion, fintech businesses have chosen a customer-focused approach. Since, they aren't as strictly monitored as regular banks, they possess a competitive edge.

Yet there are two sides to the fintech coin: Despite technology has made money easier to access, it has also resulted in increasing theft. These service providers gain a large quantity of financial information, as well as other sensitive personal information such as biometric data, health data,

[2]"Global Financial Stability Report"<https://www.imf.org/en/Publications/GFSR> accessed 9 November 2023.
[3]"P1730060bfa4c60010b833091f0f2fe2fc8.Pdf"<https://documents1.worldbank.org/curated/en/099735404212273637/pdf/P1730060bfa4c60010b833091f0f2fe2fc8.pdf> accessed 9 November 2023.
[4]'Eklavya Gupta, The future of Fintech in 2023,Times of India (26 January,2023) https://timesofindia.indiatimes.com/blogs/voices/the-future-of-fintech-in-2023/

and transaction details. Unluckily, the duties of protecting users from such deceptive operations fall disproportionately on customers, ignoring the structural cracks in digitalization[5]. These firms collect a large quantity of data, and the electronic format of the data allows it to be simpler to access individual's personal information. The Reserve Bank of India ("RBI") has emphasized fintech in response to these mounting concerns. It has compelled businesses to adopt a compliance-centric model to comply with RBI regulations and laws.

2. Research Problem

The pertinent issue in conducting the research is to draw the attention of readers to the grey issue India was lacking behind the codified data protection laws. General Data Protection Regulations which was issued by *"The European Union and the Information Technology Ac,t 2000"* was the important legislation for data privacy along with certain bills was there like *"DISHA"* etc. The main issue that arises over here in Data Localisation for Fintech industries is national safety and security. As financial data is essential for a country's economy, its abuse possesses the capacity to bankrupt economies. Considering the emergence of the digital economy, financial security concerns regarding data are real, and India is working on improving its infrastructure to protect it. The authors would like to contemplate with the *"National Digital Personal Data Protection Act, 2023"* how the law evolved through different stages of the bill and how it is in the current Act. Of course, it draws parallels to RBI regulating data localization for Finance Data.

3. Significance of the study

The authors gave an insight into the very well-known concept of Data regulation mechanisms for fintech industries. The authors are moving towards one of the most debatable issues i.e., Data Localization. When we're talking about data localization the first and foremost thing that comes into our mind i.e., *"Storage of confidential data"* Now the concept of Data localization has a lot of fallacies, which include the amount of security for data provided is going to be determined by the successful implementation of its data protection legislation, an expectation that India does not yet meet. As a result, RBI issued a circular for the protection of payment systems within Indian borders. The significance of conducting the analytical study for this research paper is to provide

[5]"Samarth Bansal, The Murky world of India's fintech scams, Live Mint (24th March 2020) < https://www.livemint.com/news/india/the-murky-world-of-india-s-fintech-scams-11584975873895.html>

a significant inception regarding the lack of Data protection for its localization of financial data and how it got amended after drawing parallel with the RBI Regulation of Finance Data.

4. Research Objectives

- To explore how FinTech has influenced the contours of the conventional banking system, an emphasis on India.
- To figure out the lacunae of the existing data protection laws and how the recent Data Protection Act can provide better protection for the privacy of data localization.

5. Research Methodology

The research paper has been formulated with doctrinal and exploratory forms of analytical study where the researchers will try to analyze the failure of data privacy protection how the data protection law evolved through different stages of the bill and how it is in the current Data Protection Act. Of course, it draws parallels to RBI regulating data localization for financial data. Data was collected through various journals, periodicals, websites, etc.

II. Overview of GDPR- Historical Approach

The European Parliament implemented the *"General Data Protection Regulation (GDPR) on April 14, 2016, and it took effect on May 25, 2018"*. It seeks to unify the EU privacy laws, influencing information about EU persons whether processed within or outside the EU. The GDPR classifies four primary data actors: the information subject, the data controller, the data processor, and third parties processing data that is not directly linked to the product or service provider. *"Non-compliance can result in fines of up to 4% of a company's worldwide earnings each year, or €20 million*[6]*."*Article 5 of the GDPR points out fundamental criteria of sensitive information processing, including transparency.[7] It seems that GDPR within the umbrella regarding security practices analyses theoretical themes such as readability, consistency, amount of knowledge handled, and transparency. The Payment Services Directive (2) (PSD2) is an essential EU statute that has a close relationship to the GDPR and covers privacy issues in the FinTech industry, specifically the provision of payment services. PSD2 encompasses payment

[6]"Linden et al. - 2020 - The Privacy Policy Landscape After the GDPR.Pdf"<https://users.cs.fiu.edu/~carbunar/teaching/cis5374/cis5374.2020/slides/gdpr.pdf> accessed 11 November 2023.

[7]"Data Protection Principles: Core Principles of the GDPR"<https://cloudian.com/guides/data-protection/data-protection-principles-7-core-principles-of-the-gdpr/> accessed 11 November 2023.

collecting techniques, constitutional justifications that enable financial account manipulation, and silent party data management. In the same way, as the General Data Protection Regulation does, PSD2 addresses user permission, data reduction, information safety, information transparency, data processor duty, and user profiling. Although PSD2 influences certain of the banking technology firms, the GDPR extends to all FinTech's.

III. India & Financial Security- Conventional Banking System to Fintech

Like the EU India was lagging in a codified Law for Data Protection. The authors in the previous sections talked about the implementation of GDPR and its historical approach. Now the authors would like to contemplate that GDPR extends their jurisdiction in India also for data protection owing to the lack of Codified laws *(before DPDA Act 2023*). Before the Data Protection Act, 2023 there're certain data protection bills were evolved. But it's a complete failure only *"Information Technology Act, 2000 ("IT Act") and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" ("SPDI Rules")* govern data protection in the financial sector in India. Furthermore, there are additional industry-specific rules, such as RBI standards, which must be adhered to protect consumers privacy. Because fintech platforms acquire huge volumes of client data, particularly personally identifiable information, the RBI expressed fears concerning security breaches. In November 2021, the RBI's Working Group issued a report tackling information security issues. Subsequently, was stated that because fintech platforms lack knowledge of financial information and banks do, they collect data regarding how customers spend their money in addition to social networking activities to produce credit scores and establish trustworthiness[8].

The IT Act has fostered a significant role in facilitating the development of digital banking applications that frequently collect sensitive data such as photographs and cell phone numbers to vex the debtors. Fintech platforms, as defined by the IT Act, are subject to data privacy rules and regulations. Issues over financial security have emerged as a result of the government's push for monetary inclusion, particularly among the unbanked population. However, regulators have failed to tackle this issue. The RBI established a Committee on Deepening Electronic Payments that released an analysis suggesting that confidentiality was more of a matter of consumer

[8]"Reserve Bank of India Reports"<https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189> accessed 11 November 2023.

awareness and knowledge of financial issues. Furthermore, it failed to emphasize the absence of codified data protection legislation in India in its data management guidelines. It is straightforward to follow wherever sensitive financial data ends up in traditional banking activities; however, it is more diligently to establish who is entitled to customer data with electronic payments. Data breaches occurred if banks expressed worry over non-banking organizations" utilization of financial information via the Unified Payments Interface (UPI) network[9]. Binoy Viswam[10], a Rajya Sabha MP, launched a Public Interest Litigation against the Centre, the *"RBI, and the National Payments Corporation of India (NPCI)"* in 2020 for permitting Amazon, Google, and Facebook/WhatsApp to participate lacking any examination. The petitioner claimed that the Big Four internet corporations violated RBI data localization guidelines by moving and keeping financial data on servers located outside of India. The RBI explained that it was the authority of the central government, never the RBI. The case is still being heard, and no more action has been taken.

IV. GDPR Failure

The GDPR ought not to serve as the only possible framework addressed by India while developing its own unique data protection legislation. The GDPR uses an unbiased consent paradigm that fails to properly safeguard information subjects" confidentiality in developing countries. Focusing on consumer consensus to handle information could help in improving liquidity, as intended by the government, but it is not a guarantee of information user autonomy. There's a danger of fraudulent utilization of biometric data and illicit dissemination of confidential information to law enforcement authorities. The burden of data protection should not lie entirely on the shoulders of consumers, especially in a developing country like India with low literacy rates. The RBI tends to reduce its interpretation of the right to privacy to just one idea of approval under its rules and regulations. This is shown by the data security requirements established in the RBI'[s Digital Lending Guidelines and the SPDI standards, which depend primarily on the customer's agreement to use particular data and to retract previous consent. In addition, the legislative sandbox framework stated that sandbox applicants must adhere to

[9]Mayur Shetty &Digbijay Mishra, Third-Party apps leaking info, claim banks, Times of India (Jan 16,2017) https://timesofindia.indiatimes.com/business/india-business/third-party-apps-leaking-info-banks/articleshow/56575783.cms

[10] Binoy Viswam v Reserve Bank of India and others, In the Supreme Court of India W.P.(C)NO. 1038 OF 2020.

current data privacy rules, which include the need to get the customer's explicit permission. It is merely a further instance of the RBI having erroneous hopes that the typical customer will not only fail to grasp complex and subtle elements of fintech, but will also offer permission according to such limited comprehension. The Puttaswamy[11] decision mentioned the GDPR framework substantially and found that authorization is only one constitutional basis for the processing of data. This was evident when the Supreme Court formulated a three-pronged test, namely legality, legitimate objective, and proportionality. Article 6 of the GDPR also establishes five legal grounds for handling data other than permission, such as contract performance, fulfilling legal responsibilities, safeguarding vital interests, tasks carried out in the public interest, and legitimate needs.

V. Privacy and Implication of Financial Data in Fintech Industries and Implementation of Data Protection Act

1. Overview of the Concept

In this part, the researchers would like to contemplate the data privacy issues and how various bills of Data protection are failing to curb the data falling under the ambit of the financial aspect. When we're talking about Data Privacy the first and foremost Judicial precedent that comes into our mind i.e., *"Justice K.S. Puttaswamy Judgement*[12]*"*where the data breaches lacunas first enlighten the readers posing a significant threat for the implementation of new Data Protection Act for financial data drawing parallel with the RBI guidelines has to be formulated. Although, concerns about confidentiality were dominating the news, Indians FinTech business thrived as an outcome of demonetization and the government's effort to increase e-payments. Financial technology, also known as FinTech, is sometimes referred to as *"technologically enabled financial innovation that might culminate in new business models, applications, processes, or products with an associated practical influence over the financial system or the distribution of financial service*[13]." The FinTech business aims to bring technology advancements towards banking and financial sectors[14]. In the context of the transaction value, the electronic payment

[11]Justice K.S.Puttaswamy V. Union of India, (2017) 10 SCC 1

[12]*Id.*,

[13]"Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities" Attention".

[14]"Security-Challenges-in-the-Evolving-Fintech Landscape.Pdf"<https://www.pwc.in/assets/pdfs/consulting/cyber-security/banking/security-challenges-in-the-evolving-fintech-landscape.pdf> accessed 13 November 2023.

sector within India is anticipated for an outcome of *"USD 700 billion before the year 2022, according to forecasts." "By FICCI, the worldwide FinTech sector is expected to be worth $45 billion by 2020, with a compound annual growth rate of 7.1%*[15]*. Naturally, to point out, security of information challenges affects the FinTech business as well. As an outcome, it is of the utmost importance to secure the consumer information given to FinTech companies while sustaining the development of the sector."*

2. Digital Confidentiality and Safety

The Srikrishna Committee stressed the value of privacy in society and culture, establishing data protection rules based on individuals' confidence in governmental bodies. The economic concept of laissez-faire governs these relationships in the United States, but courts acknowledge the Right to Privacy. The United States has sector-specific legislation governing privacy and data use by private businesses, but the European Union leads the world in laws about data protection, notably the *"EU-GDPR 2018*[16]*."""EU"s approach to data protection is centred on respecting individual privacy and dignity. Srikrishna Committee also emphasized that the Indian citizen-state interaction is distinct from those enjoyed by the United States or the European Union, since the Indian Constitution sees the state as an agent of human progress, with procedures established for avoiding abuses*[17]*".* The "Indian definition of privacy as an inherent right tends to be an expression of liberty beyond a restricted realm, with regulators" choices subject to court scrutiny in cases of in-proportion actions or intrusion on people's freedoms.

3. Framework for Regulation for Financial Technology

In India, the FinTech industry is governed by numerous authorities, including the *"RBI and Securities and Exchange Board of India for securities market intermediaries, the Insurance Regulatory Development Authority for insurance regulations, and Telecom Regulatory Authority*

[15]Komal Gupta Prasad Gireesh Chandra, *Panel to Find Ways to Make Business Easier for Fintech Firms*, MINT (2018),https://www.livemint.com/Politics/wcouR2gV2KJzzoQuezNxYK/Government-sets-up-panel-on-Fintech-to-make-regulations-more.html (last visited Nov 13, 2023).

[16]"What Is the GDPR? Everything You Need to Know"<https://www.digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection> accessed 13 November 2023.

[17]Global Legal Group, "International Comparative Legal Guides" (*International Comparative Legal Guides International Business Reports*) <https://iclg.com/practice-areas/fintech-laws-and-regulations/india> accessed 13 November 2023.

of India for telecommunications Regulatory systems"[18]. Fintech enterprises are frequently controlled by multiple jurisdictions. According to the *"Working Committee Report, fintech businesses are regulated under the scope of "payment systems" and require RBI permission.* "Henceforth, the RBI has the authority to provide instructions to payment systems and system participants[19]; tools RBI can utilize for issuing instructions. The *"payment and Settlement Systems Act of 2007 and the Payments and Settlement System Regulations of 2008"* govern the process of payment space. Furthermore, the *"RBI regulates the administration of peer-to-peer financing utilizing P2P master directions, which require P2P Non-Bank Financial Company to register with RBI".* Furthermore, the RBI has acknowledged its obligation to boost consumer trust in electronic payments by launching the ombudsman's system for electronic transactions (OSDT) as an issue resolution tool.

4. Security of Personal Data and Privacy Regulations within the Fintech Industry

Under *"Section 43A of the IT Act,"*RBI has issued notifications to govern privacy and data protection in the Fintech business, with an emphasis on the transmission of highly confidential personal data. The RBI has stressed the importance of strong stand-alone data privacy regulations to maintain consumer trust in the financial technology sector and safeguard citizens from unlawful use of personal information. The Working Committee has advised that data be classified by its importance and potential exposure, while FinTech organizations must establish secure transactional rules for security, reliability, and accessibility. RBI also urged that all FinTech organizations create a Network Management System and establish procedures to safeguard the security of Daktari has also stated that FinTech businesses shouldn't be utilized for outsourcing financial institution functions and that credible threats must be identified. The existing data protection regime is overseen by a legally binding agreement between the parties, without users having little to no say in the conditions of the agreement.

[18]"Report of the Steering Committee on Fintech_2.Pdf"<https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech_2.pdf> accessed 13 November 2023.

[19]"WGFR68AA1890D7334D8F8F72CC2399A27F4A.Pdf"<https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF> accessed 13 November 2023.

VI. Data Protection Regulation Framework- Drawing Parallel to RBI Directive

As we know, data is an ever-growing asset. Data is all around us throughout our daily conduct. In the 21st century, data has become an indispensable part of our lives as technology develops, and potential use and misuse of data are yet to be discovered. However, the significant misuse of data reflected in the corporate world has an impact on the right to privacy[20]. Therefore, it became essential to protect valuable data and introduce safeguards to achieve this goal. In India, the concept of data was introduced through the *"IT Act, 2000 under section 2 (1) (o)"* as *" a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and intend to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer"*[21]. India has implemented the requisite legislative frameworks to instil a strong sense of confidence among its inhabitants over the management of sensitive information by the government, business community, and private enterprises. Henceforth, is indisputable that Indian data protection interpretation has been a protracted battle against intricate information issues related to privacy. The Indian Supreme Court established the basis for data protection law whenever it concluded that establishing the right to privacy constitutes a fundamental right. However, it cannot deny that Indian jurisprudence on data protection laws has been a long struggle against complex issues of informational privacy. *"The Supreme Court declared the Right to privacy a fundamental right and became the foundation of data protection law in India."*

The Indian data protection framework evolved over the years, initially with the *"Introduction of the IT Act, 2008 amendment, the Sensitive Personal Data and Information Rules, 2011, "Puttaswamy judgment in 2017[22]", The Personal Data Protection Bill, 2019, The Draft Digital Personal Data Protection Bill, 2022 and the Digital Personal Data Protection Act, 2023".* The authors will analyze and point out the loopholes in the bills over the years and whether the

[20]Journal of Legal Studies and Research, "Driving Data: A Study On Data Protection & Privacy Laws" (*The Law Brigade Publishers (India)*, 22 July 2020) <https://thelawbrigade.com/cyber-law/driving-data-a-study-on-data-protection-privacy-laws/> accessed 21 November 2023.
[21]The Information Technology Act, 2000, sec:2(1)(o).
[22]Puttaswamy., supra note 10

"*Digital Personal Data Protection Act"* has received success as it overcomes the shortcomings of privacy losses.

1. Information Technology Framework

It primarily focused on electronic trade and did not address the issue of misuse or manipulation of data. It is based on financial protection in the online transaction sector. In 2008, *"section 43A and 72A was added to safeguard an individual against the dangers of processing or storage of sensitive personal data by the corporate bodies."* Following the *"Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011"* addresses the absence of 2008 amendment to specify what was meant by sensitive personal data or information. Under *"section 43 A of the IT Act, 2000"*, the authority was given to the government to bring regulations and give a thorough description of sensitive personal data. It argues that the definition was narrow in comparison to GDPR.

2. Landmark Precedent- K.S Puttaswamy Analysis

Retired Justice K.S. Puttaswamy[23] filed a petition to draw attention to Indians data privacy policy. *"It held that the right to privacy is part of the Right to life and personal liberty under Article 21 of the Indian Constitution. However, the right to privacy was not absolute in nature, and reasonable constraints were given based on legality, need, and proportionality."* This judgment lays the foundation of data protection law in India. A report was given by the *"B.N. Krishna Committee in 2018",* leading to the *"Personal Data Protection Bill, 2019 in compliance with GDPR". "The recommendation of the Srikrishna Committee has made it compulsory for the data localization[24] of all sensitive personal data. RBI's circular of 6th April 2018 has categorized "sensitive personal information"* which has prohibited transfer and processing outside India. The RBI Circular has forced payment system companies to modify business models to store data locally. The reason behind the mandate of data localization is national security and wealth creation. The basic concept of localization is the fact that citizen's data belongs to the country where it is generated and should be stored in that country's territory. Regarding national wealth creation, it is evident that financial data provides the information for customer profiling needs for targeted advertising and campaigns. It is also a growing concern

[23]Puttaswamy., supra note 10.

[24]'Data Localisation and Its Effects on Fintech Industry | Lokniti' <https://mpp.nls.ac.in/blog/data-localisation-and-its-effects-on-fintech-industry/> accessed 21 November 2023.

that multinational fintech firms have started operating in India and avoid taxes by taking advantage of the loopholes in the legal framework. Data localization would be the answer to curb the loopholes. Data localization would lead to the advancement of economic growth and the generation of tax revenue.

3. Personal Data Protection Bill, 2019

The regulation is intended for oversight over the treatment of people's data by the judiciary, corporate authorities, and entrepreneurs in India and overseas. It should be mentioned that data collection was permitted if the subject provided consent. Allowances allow for specific types of data processing under the regulation. The provision had certain loopholes that eventually led to the withdrawal of the provision by the government. The provision raises an obligation on data fiduciaries to collect data fairly and reasonably for personal data processing. What is fair and reasonable manner was not specified. It hampered the availability of proper data infrastructure and led to poor data localization by smaller organizations. A discretionary power was given to the data fiduciary to generate reports of security breaches along with assessing if the information leak affected the data owner. It can be a biased approach since data fiduciaries might not report relevant data breaches to escape from liability under the Bill. Various terminologies were introduced without any meaning given; serving a copy of data, critical personal data, and its ambit was not specified. Moreover, the bill gave the government access to non-personal data. It should have been dealt with in a separate bill. It led to access to commercial information, corporate intellectual property, corporate trade matters, mergers, and acquisitions. A brief analysis led to sections[25] 14, 13, 19, and 20, which show measures in the government's interests and give it, the ability to obtain private data of its residents under the pretence of public good. It also laid down exemptions of certain laws for specific processing of personal data where standards of necessity as laid down in Puttaswamy' s judgment was not complied with.

4. Digital Data Protection Bill, 2022

Over the years personal data protection bill have been introduced in India in compliance with the GDPR. It has to analyze *"whether GDPR is the standard for India. It hopes that the DPDP Bill 2022 will fill the gaps in the 2019 Bill"* still comes up with more ambiguities. Specifically, it says that businesses must provide reasonable means of security for personal data. It does not

[25]Puttaswamy., supra note 10.

specify what the reasonable means are. Similarly, the terms "likelihood of risks of rights and freedoms, undue delay may still need clarification[26]. Numerous provisions of the bill are affected by arbitrariness. Section 8 of the Bill introduced the concept of Deemed consent in certain situations, for example when the user voluntarily gives personal data, when it's a court order, medical emergency, epidemics, disasters, employment, public interest, and fair and reasonable cases. The lack of clarity in what is deemed consent in certain situations gives the government the liberty to operate without much transparency. It leads to discriminating use of powers and violates Article 14 of the Indian Constitution. *"Under section 18(2), the Central Government can exempt any instrumentality of the state from compliance with the law. It gives immunity from the application of law and leads to infringement of the right to privacy under Article 21 of the Constitution. The provisions are vague in such situations. "The Data Protection Board of India was introduced by the Bill. The members of the Data Protection Board are appointed by the central government only."* It is an excessive delegation of power to the Central Government since the selected terminology and conditions of employment are to be determined without any set guidelines in the provision, violating the Rule of Law under Article 14. Due to certain shortcomings of the provision, there was a need to bring a better legal framework.

5. Digital Personal Data Protection Act, 2023

"*The Bill was introduced by Lok Sabha on 3rd August 2023 and unanimously by Rajya Sabha on 9th August 2023 and received presidential assent on 11th August 2023.*" As we have pointed, previous Personal Data Protection Bills of 2019 and[27] 2022 lagged and had several gaps regarding data localization, compliance, and transparency. The said provision is supposed to fill those gaps. As opposed to IT Rules, the EU"s GDPR, the Digital Personal Data Protection Act covers all forms of personal data. It did not classify, the data into sensitive or critical groups. However, it is clear as to the obligations of the entities in the Act, but unclear of the stored data before the Act. It is unclear, how the businesses, have collected harvested or used the data before the enactment of the Act. Therefore, a comprehensive data report should be prepared by the businesses since the data could involve individual identification, medical history, web history, and financial information only in digital forms.

[26]'Digital Personal Data Protection Bill, 2022'.

[27]Ishwar Ahuja Kapadia Sakina, 'Digital Personal Data Protection Act, 2023 – A Brief Analysis' (*Bar and Bench - Indian Legal news*, 22 August 2023) <https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis> accessed 21 November 2023.

Applicability: The legislation applies to the processing of personal data in India, including both online and electronic traditional info, and it will additionally apply to the processing of information outside of India. The Act is the first administration statute in India to use she/her while referring to persons. The Act would apply to the processing of digital personal data in both digital and non-digital forms.

Consent: The significant change brought by the Data Protection Act of 2023 is consent. As per *"section 6 of the Act, personal data can be processed only for a specific purpose and only after obtaining consent from the Data Principal. It mentions that such consent has to be free, specific, unconditional, informed, and unambiguous with clear affirmative action. However, it observes that the state or any instrumentality of the state is empowered to retain personal data or even reject any request made for the removal of personal data."*

Rights of data principals: Individuals whose data is taken for processing can access information about the processing and request corrections or deletions.

Data Transmission: Concerning the transmission of *"personal data outside India, section 16 has allowed the extraterritorial processing and transfer of personal data. Exceptional in countries where the governing body forgoes to enforce limitations by an announcement."* Many Fintech companies have enterprises operating internationally. It necessitates the transfer of cross-border data. The provision would allow such transfers, but limited to specific countries. The fintech firms who engage in international operations must closely monitor the countries listed as restricted and even ensure their data transfer practices comply with the provisions of the legislation.

Impact on different sectors: Through the implementation of the latest legislation, companies, including businesses that manage personal data in any way, would now be required to establish a routine of operations and train their employees to meet certain requirements, such as collaborating with the data protection officer as and when selected by a significant data trustee. According to *"section 10 of the Act, concerning data localization, the Act has necessitated evaluation of the interplay between the Act and the sectoral regulations, especially the fintech sectors."* Financial sector guidelines were progressive by establishing legislation for safeguarding specified data and measures such as localization, in addition to providing a

framework for technological innovation in banks and NBFCs. According to the Act, the fintech and crypto enterprises are classified as data fiduciaries[28]. As we know such enterprises rely heavily on the handling of sensitive financial as well as personal data, which will impact their practices. It emphasizes obtaining explicit consent, transparency in data processing, and safeguarding of personal data in alignment with the fintech companies. It could even lead to adjustments in their user consent mechanisms and data protection protocols[29]. The financial sectors trustees can assess the internal policies and methods governing the disclosure and exchange of sensitive information, and they can also the companies that handle that process on their behalf. The statute makes no mention of particular grounds for processing. With believed approval, there is absolutely no mention of public interest or fair and reasonable goals. The Act allows processing for a fiduciary-specified purpose in which the information principle has willingly provided personal information and whose permission has not been rejected.

Fintech enterprises are entrusted with safeguarding users financial data from unauthorized access and breaches. Therefore, the Act has made it mandatory to report data breaches to the Data Protection Board of India and is relevant for fintech companies. The Act has made it an obligation to inform the data principal, the Data Protection Board, to CERT-In in case of a data breach. Failure to comply would lead to hefty monetary sanctions that range from anywhere between INR 10,000 to INR 250 Crores.[30] This is one of the highest financial penalties ever mentioned in the evolution of data protection laws in India.

Therefore, it is time for businesses to consider subjecting to encryption, and anonymization to reduce the chance of data breaches and mitigate the risk of data breach. However, when it comes to compliance, it would lead to increased operational expenses. Fintech companies specifically start-ups with limited funds may have to re-think their budgets for legal consultations. Fintech enterprises even thrive on innovation and customize financial services that are based on user data insights. Therefore, a balance between data protection and innovation is the crucial point now.

[28]"Navigating the Digital Personal Data Protection Act, 2023: Unpacking Its Impact on the Fintech Landscape | NovoJuris"<https://www.novojuris.com/thought-leadership/navigating-the-digital-personal-data-protection-act-2023-unpacking-its-impact-on-the-fintech-landscape.html> accessed 21 November 2023.
[29]Edul Patel, The Impact of India's data protection Bill on fintech, https://www.cioandleader.com/article/2023/09/11/impact-indias-data-protection-bill-fintech#1 (Last visited 20 Nov, 2023).
[30]*Id.*

Fintech firms have to explore and find ways to offer services adhering to data privacy principles and mechanisms to ensure data localization side by side. So, it is evident that organizations of different sectors focussing on the financial sector or fintech have to re-evaluate their data protection[31], data localization, and transparency practices and fill all the gaps to stay on the right path. It assists the present Act of data protection as a deterrent form of regulation. The Act has enormous potential to reshape the world of fintech in India. There are challenges regarding compliance, new consent strategies, security, and reduction of data breaches. The fintech industry has to reinforce user trust strengthen its cybersecurity measures and align its operations with Indians ever-evolving data protection frameworks.

Conclusion:

Finally concluding, authors discusses all the pertinent issues arising with data localization by drawing parallel with RBI Directive Guidelines. The authors over here evaluate three sets of issues, which really impedes the privacy of data. Firstly, there has been a claim that local processing of data would strengthen its security and confidentiality by guaranteeing that the data is properly safeguarded. Second, it suggests that an absence of governmental access to information (due to its storage in another jurisdiction) impedes the state's law enforcement and regulatory activities, could be solved by localization.

Third, there is a narrative about the financial benefits of national business, such as the creation of regional information infrastructure, employment, and contributions to the AI environment. The authors identified the precise issue that is intended to be solved, in addition to the facts revealing the extent of the issue. It seems prudent not to issue any broad directions on localization, whether for classes of personal data or contrary until a more thorough investigation of the issues at hand has been completed. Additionally, India must reject pressure to engage in bilateral or multilateral trade agreements that restrict its capacity to make future decisions on data localization in specific, or its deeper position on e-commerce in general. India's stance on data localization must eventually be weighed against the government's ambitions to establish a "Digital India," as well

[31]"Decoding the Digital Personal Data Protection Act, 2023"<https://www.ey.com/en_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023> accessed 21 November 2023.

as the need for strategic consideration of whether a closed or open-source data sector might be more suited for accomplishing those objectives.

NAVIGATING LEGAL SAFEGUARDS IN BANKING'S DIGITAL ERA

- *Pragya Sinha & Ankita Rajkumar Gupta*[1]

Abstract

The rapid evolution of technology has revolutionized various sectors, including banking and finance. However, alongside its benefits, technology brings forth the curse of cybersecurity threats. Confidential data has become a valuable currency, demanding cautious handling to prevent security breaches and reputational damage. The expanses of cyberspace and the anonymity of the dark web pose substantial challenges, necessitating robust cybersecurity measures.Cybersecurity is essential in safeguarding systems, networks, and software from digital attacks like malware, phishing, and insider threats targeting sensitive data. Our reliance on technology in daily life renders us vulnerable to advanced malware, disrupting devices and livelihoods. Thus, the need to protect personal information gives rise to the concept of cybersecurity. As society evolves and crimes adapt, stringent laws and their rigorous enforcement become imperative, especially in the banking sector. The fusion of cyber finance and legal aspects demands comprehensive safeguards. As financial institutions heavily rely on technology, creating adaptive regulations becomes crucial to anticipate and address current and future threats. International collaboration is essential due to the global nature of cyber threats. Legal frameworks should cover data protection, incident response protocols, and liability to ensure accountability during cyber breaches. Continuous legal updates are vital to match the pace of evolving technology and tactics employed by cybercriminals. The synergy between legal and cybersecurity measures is pivotal in establishing a resilient and trustworthy foundation for digital financial transactions. Balancing innovation with regulation is key to fostering a secure environment in the era of cyber finance.

Keywords:*Cyber-Security, Cyber-Finance**, Fin-Tech, Banking-Frauds, Socio-Economic Impacts**.***

[1] LLM, NiSM [National Institute of Securities Market], Gmail: pragya29sinha@gmail.com, law.duniya@gmail.com.

I. Introduction

In the development-prone world, we have seen many advances in science and technology which has helped in upliftment of various sectors like Banking, Finances, Securities Market and many more.[2] But time is a thief. With the ticking time, the curse of technology came lingering behind the benefits and advances of the same. As we know confidential data and information are the new currency and gold it needs to be used carefully. If not, this can harm the security and reputation of one.

Cyberspace, is like an area with no boundaries. It is an environment, where computer networks communicate with each other. On the other hand, there's a dark web where users operate the web anonymously.[3] These all are the challenges faced by various sectors due to which they need cybersecurity.

Cybersecurity, is the measure to protect system, network, and software programmes from cyberattack i.e. digital attack such malware, phishing, insider threats, spoofing, etc.[4] These attacks generally target the unauthorized retrieval, modification, or destruction of confidential data.[5]

Life in today's world can't be thought of without the involvement of technology. We wake up by an alarm, wear a smartwatch to calculate our steps, work on our personal computers and laptops and are able to handle our various important personal and professional lives by being dependent on technology. This dependency often leads to vulnerability to the new and advanced technology malwares disrupting our devices and tech-run appliances eventually making our life miserable.[6] Thus, with change in needs and development of the technical environment at such a fast pace, there is a requirement of safeguarding our personal and private information. Thus, comes the concept of Cyber-security.

[2]*Financial Technology (Fintech): Its Uses and Impact on Our Lives*, (Apr. 27, 2023), https://www.investopedia.com/terms/f/fintech.asp. last visited 19 August 2023.
[3]*ScienceDirect*, https://www.sciencedirect.com/science/article/pii/S2352484721007289. last visited 19 August 2023.
[4]*What is cybersecurity?*, https://www.ibm.com/topics/cybersecurity. last visited 18 August 2023.
[5]Mary K Pratt, *Cyber Attack*, (Aug. 24, 2022), https://www.techtarget.com/searchsecurity/definition/cyber-attack.
[6] https://www.sciencedirect.com/science/article/pii/S0022000014000178 last visited 18 August 2023.

Cybersecurity has a direct impact not only on an individual, but also to our society in various ways,[7] some of which are as follows: -

- Protects individuals and organizations.
- Prevent data breach.
- Identity theft.
- Maintain trust of Customers and Employees.

Challenges faced

The majority of sectors are connected via technology and hence, almost all the sectors are prone to cyber-attack including defenses, IT sector, hospitals, Government, etc. From small to large enterprises, from one small least developed country to massive developed countries, all are facing cyber security challenges.[8] Few major challenges are mentioned below:

- ➢ The attacker creates such a type of software where the virus penetrates the system so smoothly that the victim is unknown about the attack done on his/her system. The system itself doesn't provide any notification.
- ➢ Ransomware attack
- ➢ Threats
- ➢ Malware attack
- ➢ Password Attack

Types of Cyber Security

Looking at the present scenario, stringent cyber security is the need of time. Cyber security can be broadly divided into the following:

- ➔ Network Security: Provides security to the connecting networks.
- ➔ Cloud Security: Store data in encrypted form.
- ➔ Application security: Aim to secure, prevent or protect data within the App.

[7] Gerhard Conradie, *Why Cybersecurity is Important for a Modern-day Society*, ENHALO (Jan. 20, 2021), https://enhalo.co/must-know-cyber/why-cybersecurity-important-for-modern-day-society/. Last visited 19 August 2023.

[8] *Cybersecurity Is Critical for all Organizations – Large and Small*, IFAC (Nov. 28, 2023), https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small.

There are many other types of cyber security as per the needs of society which keep on updating or cyber securities get new products in market to safeguard the customers from the shadow hackers and cyber attackers.

II. Indian Laws Protecting its citizen against Cyber Crime

1. Information Technology Act, 2000

The Information Technology Act, 2000 in India protects citizens against cybercrime by legally recognizing electronic transactions, prescribing penalties for offenses like unauthorized access and data theft, safeguarding data privacy, and establishing a Cyber Appellate Tribunal. The Act also shields intermediaries from liability while imposing obligations to remove unlawful content. Additionally, it validates digital signatures and sets up adjudication authorities to handle cybercrime disputes, contributing to a legal framework for electronic transactions.

2. Indian Contract Act, 1872

The Indian Contract Act, 1872 doesn't explicitly target cybercrime, but applies to online contracts. It provides a legal framework for agreements, specifying their formation, breach consequences, and available remedies. While offering general protection for contractual relationships, its provisions may be invoked in cases of cyber-related breaches.

3. Indian Penal Code, 1860

The Indian Penal Code, 1860, protects Indian citizens against cybercrime by incorporating provisions that criminalize offenses such as hacking, identity theft, and online fraud. Sections 43, 66, and others specifically address unauthorized access, data tampering, and cyber fraud, imposing penalties. This legal framework aims to deter and punish cybercriminals, enhancing the overall protection of citizens in the digital space.

4. Cybersecurity in Banking

Cyber Securities are meant to guard against virus, hacking, malware, attack, cyber theft, digital attack, unauthorized access in networks and data. In today's world cyber security is a must in each sector because each sector has been upgrading itself on digital and technical parameters.
In thIS article the author will be discussing cyber security in banking sector.[9]

[9] Kavitha Srinivasulu, *Cybersecurity threats in digital banking sector*, (Aug. 1, 2023), https://cio.economictimes.indiatimes.com/news/digital-security/cybersecurity-threats-in-digital-banking-sector/102298156.

Banking as an important growing sector has digitized itself in many forms like one can transfer amounts electronically, can check the balance sitting on one's couch, can pay digitally, apply for loan, pay bills, and many other tasks can be done.[10]

Cyber security can safeguard online financial activities done through banks. It will check on the networks, threats, regulatory activities, encryption, storage of data and other risk management.

Many laws get enacted based on social circumstances and conditions. India, the land of many laws and regulations, has maintained its own security by many legislatures. India ensured the cybersecurity and securities of the banking system through various legislature: -

The Information Technology Act, 2000,[11] Deals with cybercrime. Its primary goal is to govern cyber law in India. The IT Act has recognized many electronic documents, contracts and transactions.

The RBI Guidelines[12]: RBI issues guidelines and various circulars to financial institutions for the precautionary measures and to understand the need of cyber securities to avoid risk and incident.

The Payment and Settlement Systems Act, 2007[13]: This Act focuses on regulating and providing supervision to the payment system in India.

The National Cyber Security Policy, 2013[14]: Build to safeguard the information in cyberspace. Prevent cyber threats. This cooperation helps to minimize the damage caused by cybercrime.

III. Banking Frauds and Role of Cyber Law

Identity Theft, where the attacker pretends to be someone else and commits a criminal act through the victim's personal information.[15]

Phishing attack is an attempt to steal confidential and sensitive information which can be utilized and can be sold on the dark web. Cyber law aids banks and other financial institutions to combat attacks like identity theft, phishing. It imposes penalties on wrongdoers.[16]

---

[10]Somer Anderson, *What is Online Banking? Definition and How It Works*, (Apr. 9, 2023), https://www.investopedia.com/terms/o/onlinebanking.asp.

[11]*India Code: Information Technology Act, 2000*, https://www.indiacode.nic.in/handle/123456789/1999.

[12]*Reserve Bank of India*, https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=900.

[13]*Reserve Bank of India - Payment and Settlement Systems Act, 2007*, https://rbi.org.in/SCRIPTs/OccasionalPublications.aspx?head=Payment%20and%20Settlement%20Systems%20Act, %202007. Last visited 18 August 2023.

[14]*National Cyber Security Policy-2013*, Ministry of Electronics and Information Technology (May 27, 2016), https://www.meity.gov.in/content/national-cyber-security-policy-2013-1. last visited 18 August 2023.

[15]Ben Lutkevich, *Identity Theft*, (Sept. 21, 2021), https://www.techtarget.com/searchsecurity/definition/identity-theft.

Insider Threats, is very common practice where a current or former employee of the company collects confidential data or misuses the access of the organization for wrongful gain this can cause various types of insider threat like malicious insider (intentionally stealing the sensitive information) and careless insider (who unknowingly exposes the details to outsider, or where an employee clicks an insecure link).[17]

Case

- Umashankar Sivasubramaniian v. ICICI Bank[18] –

  Mr. Umashankar, the complaint, claimed that the bank's incompetence resulted in an unauthorized deduction from his bank account. The Bank argued that the issue dealt with phishing, accused the complainant of being negligent, and held that the complaint must file a formal complaint in order for the case to fall under the ambit of the IT Act. In an order, the adjudicating authority found that ICICI Bank had not demonstrated that reasonable precautions were taken to prevent the breach, found the bank guilty of the offenses listed in Section 85 read in conjunction with pertinent provisions of Section 43 of the IT Act, and ordered ICICI Bank to make a payment to the complainant in the amount of Rs. 12,85,000/- (Rupees Twelve Lakh Eighty-Five Thousand only) to the complainant. A stay had been granted to the bank, and the Cyber Appellate Authority had been notified of the appeal.

- Mphasis BPO Fraud (2005)[19]:

  Four Mphasis workers at an outsourced facility in India were able to collect PINs from four U.S.-based clients of the company in December 2004. They opened new bank accounts under bogus identities using information they got, even though they were not allowed to do so. Instead, they pretended to be in charge. In a few months, they utilized the login credentials to move all of the clients' funds from their American bank accounts to their new accounts at Indian banks.

  The U.S. bank had alerted the Indian authorities to the scam by April 2005, and following an inquiry, those responsible were taken into custody. It was reported that $230,000 of

[16]*Phishing Attack: 6 Types of Phishing and How to Prevent Them*, https://www.bluevoyant.com/knowledge-center/phishing-attack-6-types-of-phishing-and-how-to-prevent-them. last visited 17 August2023.
[17]Andrew Froehlich, *Insider Threat*, (July 22, 2022), https://www.techtarget.com/searchsecurity/definition/insider-threat.
[18]Umashankar Sivasubramaniian v. ICICI Bank(Civil Petition No. 2462/2008)
[19]*Pune Citibank Mphasis Call Center Fraud*, (Oct. 5, 2019), https://www.slideshare.net/RishabhChokshi/pune-citibank-mphasis-call-center-fraud.

the $426,000 that was taken was recovered. The thieves attempted to take money out of the Indian bank account, but the arrests were successful. The Court determined that since the offense involved gaining unauthorized access in order to carry out fraudulent operations, Section 43(a) applied.

IV. Unseen Juridical Currents

1. Emerging Trends and Technologies in Banking

The banking sector is undergoing significant transformations with the advent of various technological trends, each presenting both opportunities and cybersecurity challenges. The growing popularity of mobile banking and the adoption of digital wallets underscore the need for strong security protocols.[20] These measures are crucial to safeguarding confidential financial data and thwarting unauthorized entry into mobile accounts. The rise of blockchain technology and crypto currencies introduces the need for safeguarding digital assets and securing transactions on decentralized networks. Cloud computing is another noteworthy trend, offering scalability and cost-efficiency, but mandates rigorous cybersecurity measures to guarantee the safeguarding of data stored in the cloud.

Open banking, characterized by increased collaboration and data sharing among financial institutions and third-party providers, poses cybersecurity challenges related to secure API implementation, data breaches, and the integrity of shared financial information. Artificial intelligence and machine learning are being integrated into banking processes for fraud detection, risk management, and customer service. However, ensuring the security of AI algorithms and protecting against adversarial attacks is crucial.

The Internet of Things (IoT) is contributing to smart banking solutions, but it introduces security concerns related to the protection of connected devices and the data transmitted between them. Biometric authentication, using fingerprints or facial recognition, is on the rise, necessitating measures to safeguard biometric data from theft or manipulation. The potential advent of quantum computing poses a unique challenge, as it could compromise existing encryption methods, requiring the development of quantum-resistant algorithms.

Addressing these challenges requires comprehensive cybersecurity strategies, including advanced threat detection systems, regular security audits, and compliance with regulatory

[20]Mahin Gupta, The importance of security in Digital Asset Wallets – How to safeguard your digital asset investments, (June 24, 2023), https://timesofindia.indiatimes.com/blogs/voices/the-importance-of-security-in-digital-asset-wallets-how-to-safeguard-your-digital-asset-investments/?frmapp=yes last visited 19 August 2023.

standards. Collaboration with cybersecurity experts and staying abreast of the evolving threat landscape are essential for maintaining the integrity and security of the banking sector in the face of technological advancements.

2. Legal Implications of Fintech Integration

Fintech Integration is the incorporation and seamless blending of financial technology solutions into existing financial systems or processes. Fintech encompasses a wide range of technologies and innovations designed to enhance and streamline various aspects of financial services. Its goal is to leverage these technologies to improve efficiency, accessibility, and the overall user experience within the financial industry.

Fintech integration gives rise to a range of legal considerations at the intersection of finance and technology. Compliance with data protection laws, such as General Data Protection Regulation, is imperative due to the vast amounts of sensitive financial data handled by fintech solutions, necessitating robust cybersecurity measures to avert data breaches. Negotiating a complex regulatory environment is crucial, encompassing financial regulations, anti-money laundering (AML) laws, and consumer protection regulations to avoid legal penalties and safeguard consumer rights.

For fintech ventures engaged in digital payments, adherence to payment regulations governing electronic fund transfers and transaction security is essential. The use of blockchain and cryptocurrencies introduces legal challenges, requiring compliance with laws related to initial coin offerings (ICOs), securities, and money transmission. Intellectual property protection becomes vital for proprietary fintech technologies, involving patents, trademarks, and copyrights to prevent infringement.

Navigating cross-border operations demands awareness of international legal frameworks, trade regulations, and tax laws. Additionally, ethical considerations, such as algorithmic fairness, pose legal risks, necessitating a proactive approach to mitigate potential discriminatory practices.[21] In this intricate legal landscape, collaboration with legal experts is

[21] Ruth Larbey, (Mar. 11, 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf. Last visited 20 August 2023.

essential for fintech companies to ensure compliance, address risks, and foster responsible innovation.

The incorporation of financial technology into the banking industry gives rise to numerous legal ramifications which reflect the evolving landscape at the intersection of finance and technology.

First and foremost, data privacy and security issues arise due to the substantial amount of sensitive financial information processed by fintech applications.[22] Adherence to the data protection regulations, such as the GDPR, plays a very important role in preventing unauthorized disclosure of data.[23]

Meeting regulatory requirements presents a substantial legal hurdle. Fintech firms must navigate an intricate network of financial regulations, AML statutes, and know your customer (KYC) prerequisites. Non-compliance with these regulations may lead to harsh penalties, legal proceedings, and harm to reputation.[24] As fintech often involves cross-border transactions, adherence to international financial laws and regulations becomes crucial, adding another layer of legal complexity.

Digital payments, a prominent aspect of fintech in banking, introduce legal considerations related to payment regulations. Ensuring compliance with electronic fund transfer rules and transaction security standards is essential for the legality and security of digital payment processes.

The use of blockchain and cryptocurrencies in banking fintech operations presents legal challenges, including compliance with regulations surrounding ICO, securities laws, and anti-fraud measures. Intellectual property concerns also arise, with fintech companies needing to safeguard their innovations through patents, trademarks, and copyrights.

Consumer protection laws must be carefully observed, especially concerning transparent communication of terms and conditions, fair lending practices, and the prevention of discriminatory practices in algorithmic decision-making.

In conclusion, the legal implications of fintech integration in the banking sector encompass a broad spectrum, from data protection and regulatory compliance to intellectual property and

[22] Anushka Narayan, *is your data safe with fintech? An analysis of india's financial data protection framework using gdpr principle*, social science research network, 2023

[23]Donal Tobin, *What is Data Privacy—and Why Is It Important?*, Integrate.io (May 19, 2023), https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/. Last visited 18 August 2023.

[24]*Anti-Money Laundering Guidance for FinTech*, Sanction Scanner https://sanctionscanner.com/blog/anti-money-laundering-guidance-for-fintech-167. last visited 20 August 2023.

consumer rights. Navigating these legal complexities requires a thorough understanding of the legal landscape, ongoing compliance efforts, and collaboration with legal experts to ensure the seamless and lawful incorporation of fintech innovations into banking operations.

V. Challenges in Implementing Legal Safeguards

Introducing legal protections for cybersecurity in the banking industry poses numerous challenges, given the sector's vital responsibility in protecting confidential financial data.[25] These challenges encompass the dynamic nature of cyber threats, the international scope of the financial industry, and the need for regulations to adapt to rapidly evolving technologies.

1. Sophistication of Cyber Threats:

The banking sector faces increasingly sophisticated cyber threats, including malware, phishing, and ransomware attacks. Crafting legal safeguards that can effectively combat these evolving threats is challenging due to the rapid evolution of cybercriminal tactics.[26]

2. *Cross-Border Nature of Cyber Attacks*:

Cyber-attack often transcends national borders, making it challenging to enforce legal measures universally. The global nature of the banking sector necessitates international collaboration and standardized legal frameworks to counter threats that operate across jurisdictions.

3. *Rapid Technological Advancements*:

The banking industry is quick to adopt new technologies, such as cloud computing and artificial intelligence, to enhance services. Legal frameworks must keep pace with these technological advancements to ensure that regulations remain relevant and effective.

4. *Data Privacy and Regulatory Compliance*:

Striking a balance between data privacy and regulatory compliance is a persistent challenge. Financial institutions must comply with a myriad of data protection regulations, and legal safeguards must provide clear guidance on how to protect customer data without hindering operational efficiency.[27]

---

[25]Tim Maurer and Arthur Nelson, The Global Cyber Threat, International Monetary Fund (2021), [https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.html]. last visited 20 August 2023.

[26]Tobias Adrian, Caio Ferreira, Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards (2023), [https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards]. Last visited 20 August 2023

[27]*Data protection regulations and international data flows: Implications for trade and development*, (Apr. 14, 2016), https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. last visited 20 August 2023.

5. ***Insider Threats*:**[28]

Internal threats, whether deliberate or not, pose a considerable risk. Crafting legal safeguards that address the human factor, including employee training and access controls, is essential to prevent internal security breaches without infringing on individual privacy rights.

6. *Resource Constraints*:

Many banks, particularly smaller institutions, may face resource constraints in implementing robust cybersecurity measures. Legal safeguards need to consider the financial capacity of different entities, ensuring that regulations are both effective and realistic for institutions of varying sizes.[29]

7. *Regulatory Fragmentation*:

Different regions and countries have varied cybersecurity regulations, leading to regulatory fragmentation. Harmonizing these regulations to create a cohesive and consistent legal framework is essential for multinational banks to navigate the complex regulatory environment.[30]

8. *Incident Response and Reporting*:

Legal safeguards must provide clear guidelines for incident response and reporting. Establishing a standardized reporting framework ensures that banks promptly notify relevant authorities and customers in the event of a cybersecurity breach, facilitating a coordinated response.[31]

9. *Public-Private Collaboration*:

Effective cybersecurity often requires collaboration between financial institutions, governmental agencies, and law enforcement. Legal frameworks must facilitate and encourage this collaboration, defining roles and responsibilities while respecting privacy and confidentiality concerns.[32]

10. Emerging Technologies:

The adoption of emerging technologies, such as quantum computing, introduces new challenges. Legal safeguards need to address the potential vulnerabilities and risks associated with these technologies to ensure the long-term resilience of the banking sector.

---

[28]*Defining Insider Threats*, CISA https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats. last visited 18 August 2023.

[29]Juan Carlos Crisanto, *Banks' cyber security - a second generation of regulatory approaches*, (June 12, 2023), https://www.bis.org/fsi/publ/insights50.pdf.lasat visited 16 August 2023.

[30]Juan Carlos Crisanto, *Regulatory approaches to enhance banks' cyber-security frameworks*, (Oct. 17, 2017), https://www.bis.org/fsi/publ/insights2.pdf. last visited 19 August 2023.

[31]*Reserve Bank of India*, https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721.

[32]*Concepts of Information Security*, https://www.nap.edu/read/1581/chapter/4. last visited 18 August 2023.

Addressing these challenges requires a holistic approach involving collaboration between regulators, financial institutions, and cybersecurity experts. Legal safeguards should be dynamic, adaptable, and informed by ongoing threat assessments to effectively mitigate cyber risks and protect the integrity of the banking sector. Regular updates to regulations, international cooperation, and a focus on balancing security with privacy are crucial components of a comprehensive cybersecurity legal framework in the banking industry.[33]

VI. Towards Enhanced Legal Resilience

1. *The Role of Regulatory Sandboxes*[34]

Regulatory sandboxes serve as innovative mechanisms that enable businesses to test new ideas and products in a controlled environment, often under the supervision of regulatory authorities. Their primary role is to strike a balance between encouraging technological innovation and ensuring regulatory compliance.

One key function of regulatory sandboxes is to address the challenges arising from the rapid pace of technological advancements that may outpace traditional regulatory frameworks. By providing a space for experimentation, these sandboxes allow startups and innovators to test their concepts without the immediate burden of full regulatory compliance. This fosters a more agile and iterative approach to development. Flexibility is a hallmark of regulatory sandboxes, offering startups the opportunity to navigate complex regulatory landscapes without being hindered by rigid rules. This flexibility encourages a culture of innovation and risk-taking, fostering an environment where new ideas can be explored without the fear of immediate regulatory repercussions.[35]

Regulatory sandboxes also play a crucial role in facilitating collaboration between regulators and the innovators they oversee. This interaction allows regulators to gain firsthand insights into emerging technologies and business models, leading to a better understanding of potential risks and benefits. Regular communication and feedback loops between regulators and sandbox participants create a dynamic learning environment for both parties.

---

[33]*Guidance on cyber resilience for financial market infrastructures*, (June 29, 2016), https://www.bis.org/cpmi/publ/d146.pdf.
[34]Editorial Team, *The Role Of Regulatory Sandboxes In Fintech Innovation*, (Sept. 10, 2018), https://www.finextra.com/blogposting/15759/the-role-of-regulatory-sandboxes-in-fintech-innovation.
[35]LOMAX Christopher, *The role of sandboxes in promoting flexibility and innovation in the digital age*, (Mar. 25, 2022), https://goingdigital.oecd.org/data/notes/No2_ToolkitNote_Sandboxes.pdf.

Furthermore, regulatory sandboxes contribute to consumer protection by providing a platform for regulators to closely monitor the impact of innovations on end-users. This proactive oversight ensures that new products and services are safe, secure, and do not pose undue risks to consumers. The sandbox experiments have also helped in developing regulations to harmonize innovation and safeguarding public interests.

In the realm of banking cybersecurity, regulatory sandboxes play a critical role in addressing the evolving challenges posed by cyber threats. The financial industry is a prime target for cybercriminals, and innovations in banking technologies must be thoroughly tested to ensure robust cybersecurity measures. Regulatory sandboxes provide a controlled environment where banks and fintech firms can experiment with new cybersecurity solutions and technologies without immediate regulatory constraints.[36]

These sandboxes enable financial institutions to assess the effectiveness of their cybersecurity measures in real-world scenarios, allowing them to identify and rectify vulnerabilities before widespread implementation. The collaborative nature of regulatory sandboxes also facilitates communication between banks and regulators, fostering a mutual understanding of emerging cyber threats and innovative cybersecurity solutions.[37]

By providing a space for testing and refining cybersecurity protocols, regulatory sandboxes contribute to the overall resilience of the banking sector against cyber threats. The iterative process within the sandbox environment ensures that cybersecurity measures keep pace with evolving cyber risks, ultimately strengthening the industry's ability to safeguard customer data, maintain trust, and uphold the integrity of financial systems.

2. Strengthening Legal Safeguards for Future Challenges

Strengthening legal safeguards for future challenges in cybersecurity involves enhancing and adapting legal frameworks to address the evolving nature of cyber threats. This is crucial to ensure effective prevention, investigation, and prosecution of cybercrimes. Key elements include:

Legislation Updates: Regularly revisiting and updating existing laws to keep pace with technological advancements and emerging cyber threats. This includes defining and categorizing

[36]Nigel Phair Director, *Sandboxing Cyber Risk to Achieve Digital Financial Inclusion Through Fintech*, Asian Development Blog (Feb. 18, 2019), https://blogs.adb.org/blog/sandboxing-cyber-risk-achieve-digital-financial-inclusion-through-fintech. last visited 17 August 2023

[37]Giulio Cornelli, *Regulatory sandboxes and fintech funding: evidence from the UK*, (Nov. 9, 2020), https://www.bis.org/publ/work901.htm. last visited 19 August 2023.

cybercrimes, outlining appropriate penalties, and ensuring the legal system can effectively address new challenges.[38]

International Cooperation: Encouraging collaboration and information-sharing between nations to combat cyber threats that often transcend borders. Establishing treaties and agreements to facilitate extradition and cooperation in investigations is vital for a global response to cybercrimes.

Data Protection Laws: Implementing robust data protection and privacy laws to safeguard individual's sensitive information. Ensuring compliance with international standards and fostering a culture of responsible data handling is crucial for building public trust.

Incident Reporting Requirements: Enforcing a mandate for organizations to promptly report cybersecurity incidents to relevant authorities promotes a coordinated response to cyber events, assists in investigations, and contributes to a comprehensive understanding of the threat landscape.

Cybersecurity Standards and Best Practices: Establishing and promoting industry-specific cybersecurity standards and best practices to guide organizations in implementing effective security measures. This can be reinforced through legal mandates or incentives for compliance.

Capacity Building: Investing in the training and development of legal professionals, law enforcement, and judiciary to enhance their understanding of cyber threats, digital forensics, and the intricacies of cyber investigations and prosecutions.[39]

Public-Private Partnerships: Encouraging collaboration between governments, law enforcement agencies, and private sector entities. This involves sharing threat intelligence, best practices, and resources to collectively strengthen cybersecurity defenses.[40]

Proactive Regulatory Measures: Anticipating future challenges and proactively crafting regulations that address emerging technologies and trends. This might include regulatory

[38]*Cybercrime Module 3 Key Issues: The Role of Cybercrime Law*, https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html. last visited 20 August 2023

[39]*National Cybercrime Training Centre (CyTrain)*, https://cytrain.ncrb.gov.in/. last visited 19 August 2023

[40]*A Shared Responsibility: Public-Private Cooperation for Cybersecurity*, https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity. last visited 18 August 2023

sandboxes, allowing controlled experimentation with new cybersecurity solutions before wider implementation.[41]

Penalties and Deterrence: Ensuring that penalties for cybercrimes are sufficiently deterrent to discourage malicious activities. This includes holding individuals and organizations accountable for their role in cyber-attacks.[42]

By continuously fortifying legal safeguards in these ways, nations can better equip themselves to face the dynamic and sophisticated challenges posed by cyber threats, ultimately creating a more resilient and secure digital environment.

VII. Potential socio-economic impacts to consider:

1. Consumer Trust and Confidence:

Positive Impact: Strengthening legal safeguards can enhance consumer trust in the banking sector, fostering confidence in digital financial transactions.

Negative Impact: If legal frameworks are perceived as inadequate, it may erode trust, leading to reduced consumer participation in online banking and financial services.

a. Financial Inclusion:

Positive Impact: Robust cybersecurity measures, supported by clear legal safeguards, can promote financial inclusion by encouraging individuals to use digital banking services, especially in regions where traditional banking infrastructure is limited.

Negative Impact: Insufficient legal protection may hinder the growth of digital financial services, particularly among populations wary of cybersecurity risks.

b. Investment and Innovation[43]:

Positive Impact: A strong legal framework for cybersecurity can attract investment in the fintech and banking sectors, leading to increased innovation and the development of secure technologies.

Negative Impact: Ambiguous or weak legal safeguards may deter investors and slow down innovation due to concerns about potential risks and liabilities.

---

[41]Nivedita Krishna, *Why India needs sectoral Regulatory Sandboxes for Artificial Intelligence based solutions*, (Sept. 10, 2023), https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/why-india-needs-sectoral-regulatory-sandboxes-for-artificial-intelligence-based-solutions/.

[42]*Cybercrime Module 10 Key Issues: Cybercrime that Compromises Privacy*, https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html. last visited 17 August 2023.

[43]Economic Times, *Invest in Innovation: What is this new investment strategy and should you go for it?*, The Economic Times (Aug. 14, 2023), https://economictimes.indiatimes.com/wealth/invest/invest-in-innovation-what-is-this-new-investment-strategy-and-should-you-go-for-it/articleshow/102669703.cms. last visited 18 August 2023

c. Economic Stability:

Positive Impact: Effective legal safeguards can contribute to economic stability by preventing cyber threats that could undermine the integrity of financial systems and markets.

Negative Impact: Cybersecurity incidents, in the absence of adequate legal protections, may lead to economic instability, affecting financial markets and investor confidence.[44]

d. Job Creation and Skills Development:

Positive Impact: Growth in the cybersecurity sector, driven by legal requirements, can lead to job creation and increased demand for skilled professionals.

Negative Impact: Inadequate legal safeguards may result in cybersecurity incidents, potentially leading to job losses and a need for retraining and reskilling.[45]

e. Global Competitiveness:

Positive Impact: A well-defined legal framework for cybersecurity can enhance the global competitiveness of the banking and fintech industries, attracting international partnerships and collaborations.

Negative Impact: Weak legal safeguards may hinder competitiveness as businesses may be perceived as vulnerable to cyber threats, impacting international trust and collaboration.

2. *Costs of Cyber-security*[46]:

Positive Impact: Clear legal guidelines can help businesses plan and allocate resources effectively for cybersecurity measures, potentially reducing the overall costs associated with data breaches.

Positive Impact: Governments may invest in cybersecurity infrastructure and legislation, contributing to national security and the protection of critical financial systems.

Negative Impact: Insufficient legal safeguards may lead to increased government expenditure in responding to and mitigating cyber threats, diverting resources from other essential areas.

Negative Impact: Lack of legal clarity may result in unforeseen costs for businesses dealing with cyber threats, including legal liabilities, reputational damage, and financial losses.

[44]Nigel Jenkinson, *Cyber Risk is the New Threat to Financial Stability*, (Dec. 7, 2020), https://www.imf.org/en/Blogs/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability. last visited 19 August 2023.

[45]Mamta Sharma, *'Critical gap': How can companies tackle the cybersecurity talent shortage?*, (Mar. 27, 2023), https://www.peoplematters.in/article/talent-acquisition/critical-gap-how-can-companies-tackle-the-cybersecurity-talent-shortage-37297. last visited 21 August 2023.

[46] Austin Gadient, *The Hidden Costs Of Cybersecurity*, (May 8, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/05/08/the-hidden-costs-of-cybersecurity/ last visited 20 August 2023.

VIII. Case Studies and Practical Insights

There have been various instances where malware and viruses have attacked systems and have led to regulatory jeopardy.[47]

Accellion, a software provider specializing in accounting software, faced a severe security breach when a zero-day exploit in its Accellion File Transfer Appliance software allowed hackers unauthorized access to the databases of numerous banks and financial institutions. Although, the cyber-attack technically occurred at the end of 2020, the repercussions were not fully realized until after the New Year.[48]

PayPal, a popular online payment platform, fell victim to a new wave of SMS-based phishing attacks in 2021, where malicious actors impersonated PayPal and lured users into divulging sensitive information through a deceptive verification site.[49]

In a separate incident involving American Express, a hacker exposed details of Mexico-based cardholders on a cybercrime forum in early 2021, claiming to possess additional data on cardholders and various banks across Mexico.[50]

Furthermore, Automatic Funds Transfer Services (AFTS), a payment processor, was targeted by the Cuba Ransomware group in February 2021, resulting in a widespread ransomware campaign that affected both state agencies in the US and the financial sector.[51]

These incidents contribute to a series of cybersecurity challenges faced by the banking industry, further emphasizing the need for continuous vigilance, investment in robust cybersecurity measures, and international collaboration to counter the evolving threats in the financial landscape. The banking sector has witnessed other notable cybersecurity incidents, including the

[47]Josh Fruhlinger, *11 infamous malware attacks: The first and the worst*, CSO Online https://www.csoonline.com/article/572911/11-infamous-malware-attacks-the-first-and-the-worst.html. last visited 19 August 2023.

[48]Josh Allen, *Accellion Data Breach: What Happened & Who Was Impacted?*, (May 31, 2021), https://purplesec.us/accellion-data-breach-explained/. Last visited 18 August 2023.

[49]*PayPal users targeted in new SMS phishing campaign*, (Jan. 4, 2021), https://www.welivesecurity.com/2021/01/04/paypal-users-targeted-new-sms-phishing-campaign/. Last visited 19 August 2023.

[50]*Credit Card Data of 10,000 American Express Accounts Posted on Darknet Forum for Free*, (Jan. 6, 2021), https://cisomag.com/american-express-credit-card-data-sale-on-darknet/. Last visited 17 August 2023.

[51]Colin Wood, *'Cuba Ransomware' attack disrupts payment providers used by state and local agencies*, StateScoop (Feb. 19, 2021), https://statescoop.com/cuba-ransomware-attack-state-local-government/. Last visited 19 August 2023.

Bangladesh Bank Heist[52], Equifax Data Breach[53], SWIFT Attacks[54], JPMorgan Chase Data Breach[55], NotPetya Ransomware Attack[56], and Capital One Data Breach[57].

These instances underscore the persistent threat landscape, emphasizing the importance of safeguarding sensitive information and financial transactions through proactive measures and global cooperation. Recently, the Indian government evaluated the preparedness of banks and financial institutions in addressing cybersecurity issues and the increasing threat of digital payment fraud. Vivek Joshi, the secretary of financial services, disclosed the suspension of seven million mobile numbers linked to suspicious transactions which is a relief.[58]

1. Practical Implications of Legal Safeguards: Successes and Failures[59]

Legal safeguards in banking cybersecurity have significant practical implications that influence how financial institutions approach and manage their security measures. Some key practical implications include:

a. Compliance Requirements: Legal safeguards often entail compliance requirements that mandate specific cybersecurity standards for banks. These standards may include data protection regulations, incident reporting obligations, and adherence to industry-specific cybersecurity frameworks. Financial institutions must invest in technologies and practices to ensure compliance with these legal mandates[60].

---

[52]Kim Zetter, *That Insane, $81M Bangladesh Bank Heist? Here's What We Know*, WIRED (May 17, 2016), https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/. Last visited 19 August 2023.

[53]*Equifax Data Breach Settlement*, Federal Trade Commission (July 11, 2019), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement. last visited 18 August 2023.

[54]*How to spot, stop and defend against cyber-attacks*, Swift https://www.swift.com/your-needs/financial-crime-cyber-security/financial-fraud/how-defend-against-cyber-attacks. Last visited 18 August 2023.

[55]Jessica Silver-Greenberg, *JPMorgan Chase Hacking Affects 76 Million Households*, The New York Times (Oct. 2, 2014), https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/. Last visited 19 August 2023

[56]Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 21, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Last visited on 18 August 2023.

[57]*2019 Capital One Cyber Incident | What Happened*, Capital One https://www.capitalone.com/digital/facts2019/. Last visited on 19 August 2023.

[58] ET Bureau, Centre checks on banks' cyber fraud readiness, The Economic Times (Nov. 29, 2023), https://economictimes.indiatimes.com/industry/banking/finance/banking/centre-checks-on-banks-cyber-fraud-readiness/articleshow/105572403.cms. last visited on 18 August 2023

[59]Chip Stapleton, *Cyberattacks and the Risk of Bank Failures*, (Mar. 23, 2023), https://www.investopedia.com/articles/personal-finance/012117/cyber-attacks-and-bank-failures-risks-you-should-know.asp. Last visted 17 August 2023

[60]*Edward Kost, Top 8 Cybersecurity Regulations for Financial Services,*UpGuard https://www.upguard.com/blog/cybersecurity-regulations-financial-industry. last visited 20 August 2023

b. *Data Protection and Privacy:* Legal safeguards necessitate robust measures for protecting customer data and ensuring privacy. Banks must implement encryption, access controls, and secure storage practices to safeguard sensitive information. Non-compliance can result in severe legal consequences and damage to the institution's reputation[61].

c. *Incident Response Planning*: Legal frameworks often require banks to have comprehensive incident response plans. This involves establishing protocols for detecting, responding to, and mitigating cybersecurity incidents. Financial institutions must invest in training and testing their incident response teams to ensure a swift and effective response in the event of a security breach.[62]

d. *Customer Communication*: In the event of a cybersecurity incident, legal safeguards often dictate the requirements for notifying affected customers and regulatory authorities. Banks need clear and effective communication strategies to manage the aftermath of a breach, which can impact customer trust and satisfaction.

e. *Cross-Border Considerations*: Many banks operate globally, necessitating compliance with various international cybersecurity regulations. Legal safeguards may require financial institutions to navigate complex cross-border data transfer regulations, harmonizing their cybersecurity practices with the laws of multiple jurisdictions[63].

f. *Vendor Management*: Financial institutions often rely on third-party vendors for various services. Legal safeguards may require banks to assess and manage the cybersecurity practices of these vendors to ensure the overall security of their operations. This involves contractual agreements, audits, and ongoing monitoring of vendor cybersecurity performance[64].

g. *Liability and Accountability***:** Legal safeguards establish liability and accountability frameworks in the event of a cybersecurity incident. Banks must be aware of the legal consequences they may face, including financial penalties and reputational damage. This

[61]*Data protection and privacy laws, Identification for Development* https://id4d.worldbank.org/guide/data-protection-and-privacy-laws. last visited 18 August 2023

[62]*Alissa Irei, What is incident response? Plans, teams and tools*, (Mar. 10, 2023), https://www.techtarget.com/searchsecurity/definition/incident-response.

[63] ITIF (July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/. Last visited 19 August 2023

[64]*Third Party Vendor Risk Management In The Banking Industry - Cybersecurity | Digital Forensics | Crypto Investigations*, Digital Forensics (Mar. 10, 2018), https://ermprotect.com/blog/third-party-vendor-risk-management-in-the-banking-industry/. Last visited 18 August 2023

awareness motivates proactive investment in cybersecurity measures to prevent breaches and minimize legal risks.

h. *Regulatory Reporting:* Legal frameworks often mandate the reporting of cybersecurity incidents to regulatory authorities. Financial institutions need to have mechanisms in place to gather and report relevant information in a timely and accurate manner, demonstrating transparency and cooperation with regulatory bodies[65].

IX. Recommendations and Best Practices-

1. Proposed Legal Framework Enhancements

Legal framework enhancements in the context of banking cybersecurity involve updating and strengthening existing laws to address the evolving nature of cyber threats. Some key enhancements include:

a. *Cybersecurity Standards and Best Practices*: Enact or update laws that mandate specific cybersecurity standards and best practices for the banking industry. These standards should cover areas such as data encryption, access controls, network security, and incident response planning[66].

b. *Incident Reporting Requirements*: Introduce or enhance laws that require banks to promptly report cybersecurity incidents to regulatory authorities. Clear guidelines on the reporting process, including timelines and the type of information to be disclosed, can improve the overall response to cyber threats[67].

c. *Data Protection and Privacy Regulations*: Implement or strengthen data protection and privacy laws to safeguard customer information. This may include defining the types of data that require protection, specifying security measures, and outlining penalties for non-compliance[68].

d. *Cross-Border Data Transfer Regulations*: Develop regulations that address the challenges of cross-border data transfers, especially for banks with global operations.

[65]*Microsoft Word - CybersecDigest_v5_July2020_FINAL.docx*, (July 26, 2020), https://pubdocs.worldbank.org/en/361881595872293851/CybersecDigest-v5-Jul2020-FINAL.pdf. last visited 18 August 2023

[66]*Banking and Financial Data Security Compliance: Requirements & Best Practices, Ekran System* (July 20, 2022), https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance. last visited 20 August 2023

[67]*Kyle Chin, Why is Cyber Incident Reporting Important?*, UpGuard https://www.upguard.com/blog/cyber-incident-reporting.

[68]*Data protection and privacy laws, Identification for Development* https://id4d.worldbank.org/guide/data-protection-and-privacy-laws.

These regulations can provide a framework for secure data sharing while ensuring compliance with the laws of multiple jurisdictions[69].

e. *Regulatory Sandboxes*: Introduce legal provisions for regulatory sandboxes that allow banks to experiment with innovative cybersecurity solutions in a controlled environment. This promotes the development and testing of cutting-edge security technologies without immediate regulatory constraints[70].

f. *Third-Party Vendor Management*: Strengthen laws related to third-party vendor cybersecurity management. This includes requiring banks to conduct thorough assessments of the cybersecurity practices of their vendors and imposing legal obligations on vendors to maintain a certain level of security.

g. *Liability and Accountability Frameworks*: Clarify legal liability and accountability frameworks for cybersecurity incidents. Define the responsibilities of banks in preventing, detecting, and responding to cyber threats, and establish legal consequences for failures to meet these obligations[71].

h. *International Cooperation Agreements*: Foster international cooperation through legal agreements that facilitate information sharing and collaborative efforts in combating cyber threats. Establish protocols for cross-border investigations and cooperation between regulatory bodies from different jurisdictions.

i. *Cybersecurity Education and Training Requirements*: Introduce laws that mandate regular cybersecurity education and training for banking professionals. This ensures that employees are well-informed about the latest threats and best practices, contributing to a culture of cybersecurity awareness within the industry.

j. *Penalties for Non-Compliance*: Increase the severity of penalties for banks that fail to comply with cybersecurity regulations. This can serve as a deterrent and motivate financial institutions to invest adequately in cybersecurity measures[72].

---

[69] *Bhavna Sharma, Data Protection Standards For Cross Border Data Transfers In India:Suggestive Approaches And Way Forward*, (May 25, 2023), https://www.livelaw.in/articles/cross-border-data-transfer-regulations-global-trade-digital-services-data-protection-229472. last visited 21 August 2023

[70] *Alyssa Abrams, Regulatory Sandboxes—a Bridge Between Regulators and Business Innovation*, Sumsub (Aug. 25, 2023), https://sumsub.com/blog/regulatory-sandboxes/. Last visited 18 August 2023

[71] Cybersecurity Frameworks 101 - The Complete Guide, Prey Blog (June 3, 2022), https://preyproject.com/blog/cybersecurity-frameworks-101.

[72] *For non-compliance with cybersecurity framework, RBI imposes Rs 65 lakh fine on bank*, (July 3, 2023), https://ciso.economictimes.indiatimes.com/news/grc/for-non-compliance-with-cybersecurity-framework-rbi-imposes-rs-65-lakh-fine-on-bank/101444656. last visited 17 August 2023

These legal framework enhancements aim to create a more robust and adaptive regulatory environment, ensuring that banks are better equipped to address the complex and evolving challenges posed by cyber threats in the digital age

X. Best Practices for Banks in Enhancing Cybersecurity Legal Compliance

Banks can adopt several practices to enhance cybersecurity legal compliance and strengthen their overall security posture. Here are key practices:

Banks can enhance their cybersecurity resilience by adopting a comprehensive approach that includes risk assessment and management. Conducting regular risk assessments helps identify and prioritize potential cybersecurity risks. Subsequently, developing risk management plans aligned with legal requirements and industry standards allows for effective mitigation of identified risks. It is crucial to implement measures to address the identified risks and continuously reassess the risk landscape to stay proactive in the face of evolving threats.

Compliance monitoring and auditing are integral components of a robust cybersecurity strategy. Establishing a thorough compliance monitoring program ensures adherence to cybersecurity laws. Periodic internal audits provide insights into compliance with regulatory frameworks, offering opportunities for improvement. Engaging third-party auditors for independent cybersecurity assessments adds an extra layer of validation.

Privacy policies play a pivotal role in cybersecurity, and banks should maintain comprehensive privacy and data protection policies in accordance with applicable laws[73]. Clearly defining the types of data requiring protection and outlining procedures for handling sensitive information are essential. Regular updates to policies are necessary to align with evolving legal requirements.

An effective incident response plan is critical for managing cybersecurity incidents. Regular updates to the plan, compliance with legal reporting requirements, and mock exercises to test its effectiveness contribute to a resilient response. Establishing clear communication protocols for notifying regulators and affected parties is essential in the event of a cybersecurity incident[74].

[73]*Data protection and privacy laws,* Identification for Development https://id4d.worldbank.org/guide/data-protection-and-privacy-laws.

[74] Paul Kirvan, *How to build an incident response plan*, with examples, template, (Feb. 3, 2023), https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan.

Supplier management is another key aspect. Implementing robust practices and ensuring third-party vendors comply with regulatory cybersecurity requirements is vital. Including cybersecurity clauses in supplier contracts establishes security standards and obligations. Regular evaluation and monitoring of third-party cybersecurity practices are essential components of a comprehensive cybersecurity strategy.

Employee training and awareness are fundamental. Regular cybersecurity training keeps employees aware of legal compliance requirements. Implementing a phishing awareness program educates employees about potential threats, fostering a culture of cybersecurity awareness and responsibility throughout the organization.[75]

Encryption and access control are technical measures that enhance cybersecurity. Implementing encryption for sensitive data in transit and at rest, along with strict access controls based on job function, contributes to a secure environment. Regular reviews and updates of access rights ensure alignment with legal and regulatory requirements.

Periodic security audits and tests, including penetration testing and vulnerability assessments, help identify and remediate potential vulnerabilities. Leveraging insights from audits and testing enables continuous improvement of the cybersecurity posture[76].

Maintaining detailed documentation of cybersecurity policies, procedures, and compliance efforts is essential for regulatory compliance. Documenting incident response actions and communications demonstrates adherence to regulations. Staying informed about changes in cybersecurity law and updating documentation accordingly is crucial.

Lastly, fostering cooperation with regulatory authorities through open communication, participation in industry forums, and seeking advice proactively contribute to a robust cybersecurity framework. By incorporating these measures, banks can significantly strengthen their compliance with cybersecurity regulations, reduce exposure to regulatory penalties, and protect themselves and their customers from evolving cyber threats.

XI. Conclusion

[75] Kinza Yasar, Security Awareness Training, Definition from TechTarget (Oct. 12, 2023), https://www.techtarget.com/searchsecurity/definition/security-awareness-training. last visited 14 August 2023

[76] *Security Audits: A Comprehensive Overview*, AuditBoard (Nov. 28, 2023), https://www.auditboard.com/blog/what-is-security-audit/. Last visited 16 August 2023

It would not be wrong to say that we live in a world which functions on technology, directly or indirectly. From work to spending time with family, technology aids everything. But as every coin has two sides, so does technology. On one hand, where it helps and eases our daily work, on the other hand, it also threatens a person's security in multiple ways. This article provides us with various issues and insights to cyber-attacks and requirements of stringent cybersecurity provisions focusing on the Banking sector.

Although, the regulatory landscape with reference to cyber-attacks has been tried to be dealt with by our lawmakers with utmost care, the present scenario suggests otherwise. Irrespective of the laws laid, there is need for proper implementation of the said rules and regulations.

With time, the need of society changes and so does the level of crimes. To deal with the cyber security threat in this world where every house has access to the internet and various A.I. tools, it is the need of time to make the laws more stringent and see to it that it is followed religiously. The government can keep on bringing new laws but if not followed can't be of any help.

The amalgamation of cyber finance and the legal landscape presents a dynamic challenge that demands comprehensive safeguards. The intricate web of financial transactions in the digital realm requires a nuanced understanding of the unseen juridical currents shaping banking cybersecurity. As financial institutions increasingly rely on technology, the potential vulnerabilities grow, necessitating robust legal frameworks.

To navigate this evolving landscape, policymakers and legal practitioners must collaborate to develop adaptive regulations that address the unique challenges posed by cyber finance. This involves not only addressing current threats but also anticipating future risks. Furthermore, fostering international cooperation is imperative, given the global nature of cyber threats in the financial sector.

The legal safeguards must encompass data protection, incident response protocols, and liability frameworks to ensure accountability and restitution in the event of a cyber breach. Moreover, continuous legal updates and advancements are crucial to keep pace with the rapidly evolving technology and tactics employed by cybercriminals.

Ultimately, the synthesis of legal and cybersecurity measures is pivotal in establishing a resilient and trustworthy foundation for the digital financial landscape. Striking a delicate

balance between innovation and regulation will be key to fostering a secure environment for financial transactions in the age of cyber finance

ACQUISITIONS IN TECHNOLOGY COMPANIES: ANALYSIS OF INVESTOR BEHAVIOUR

- *Ashutosh Chandra*[1]

Abstract

When a company is a technology company, then the priorities and risk factors of an investor change. This is because of additional considerations related to technology. Therefore, the process of due diligence, which is undertaken during acquisitions changes too. As such, corporate compliances still have an importance. But the future of company in such cases becomes centered around the technology and therefore, it is imperative to give importance to other factors. Accordingly, this paper identifies key areas that must be given importance in a due diligence. As per the author, these factors include the veracity of technology, licenses relating to the technology, standard of cyber security followed, employees, server maintenance, access, data guidelines and international compliances. While these areas are not exhaustive in nature and technology law will necessarily evolve to keep up with the growth in Information Technology sector, the casing of mentioned areas still stands essential to do proper justice to an investor. This paper goes into depth of each area mentioned and points out additional compliances required. Usually, after risks have been identified in accordance with the mentioned areas, changes also need to be made to the deal structuring aspect. The investor will be motivated to negotiate differently for rights related to the company once more risks come forward. For the most part, the considerations in representations and warranties that an investor asks will change. Finally, the paper will demonstrate that the lawyer of tomorrow, and effectively today, need to change the way they investigate technology companies and adapt to changing circumstances.

Keywords *– Acquisitions, Technology Companies, Compliances, Due Diligence, Negotiation*

[1] 5th Year, Jindal Global Law School. Gmail: Ashutoshchandra081@gmail.com

I. Introduction

When it comes to the law in the Indian jurisdiction, Section 2(20) of the Companies' Act defines a 'company' as a "company incorporated under the Act or under any previous company law." For better or for worse, the definition neither brings any clarity as to what the prerequisites are for the formation of a company, nor entails its functions. In simpler and agreeable terms, a company can be defined as an association of persons coming together to achieve a common objective.[2] More recently, there has been a change in the working of companies, or businesses in general.

Today, technology has revolutionized businesses, almost to a point where companies either need 'to adapt or die'. Companies like *Netflix* or *Amazon* serve prime example of a shift from a physical model to one centered towards technology. One of these companies started as a rental store and the other as a bookstore. Of course, these companies serve examples of the first movers in the tech space. As a result, they managed to amass huge following and usage. But, the bottom line is, technology is here, and innovation is not stopping anytime soon. New technologies are developing rapidly, and businesses are on top of their game to monetize such technology. This leads us to the famous notion that "all companies are going to be technology companies in future". Going one step further, the future is now, and technology companies have already cemented themselves on top of all tables. For one statistic, the top 5 leading companies today by market capitalization are technology companies.[3]

Given the background, there are multiple transactions that private companies often go through concerning its shares or assets in a commercial context. The reasoning for entering such transactions is not dissimilar to those adopted by traditional companies. For the process of acquiring or investing through private placement, investors or acquirers may often conduct their own investigation before entering into agreement or contract with the company or the selling party. Such investigation is referred to as due diligence. Traditionally, a legal due diligence is an investigation of legal risks related to corporate compliances, status of assets, intellectual

[2] "Taxmann, '*What is a Company*?' TAXMANN (22 November 2022) https://www.taxmann.com/post/blog/what-is-a-company-definition-characteristics-and-latest-case-laws/" last visited 18 August 2023.
[3] "THOMSON REUTERS, '*All companies are technology companies now'* (last visited 21 March 2018) https://www.thomsonreuters.com/en-us/posts/news-and-media/all-companies-are-technology-companies-now/" last visited 18 August 2023

property, real estate, and pending litigation against the company. However, when the company becomes a technology company and has 'tech' as a focal point, it is argued that the priorities and risk factors for an investor change. As such, corporate compliances still have an importance. But, the future of company in such cases becomes centered around the technology and therefore, it is imperative to give importance to other factors. This paper will argue that factors of veracity of technology, licenses relating to the technology, standard of cyber security followed, employees, server maintenance, access and data guidelines become much more important considerations. Finally, the paper will demonstrate that the lawyer of tomorrow, and effectively today, need to change the way they investigate technology companies and adapt to changing circumstances.

II. Preliminary Talks and Due diligence

In acquisitions by companies or persons, parties cannot suddenly decide that they want to become associated and complete the procedure instantly. There are a series of steps followed before the process comes into fruition. Firstly, there are preliminary contacts and talks between the parties. Here, the parties case each other in case they want to enter a transaction. Lawyers are not typically involved in the process and the parties try to formulate a term sheet which would set out the terms of the merger and acquisitions. The document is generally not enforceable, the exceptions being certain clauses of the same. Then, there is a due diligence process for identifying risks associated with the companies. The need to do a due diligence arises from Section 16 of the Sale of Goods Act due to the fact that the law does not provide for any implied warranty or condition regarding the quality or the fitness of the goods supplied under a contract of sale. Therefore, there is a need to include specific representations and warranties in a contract for them to be enforceable and this can only be done when the risks associated with them are identified.

Each due diligence is done differently based on the facts of each case. The overall goal of the parties is to try to minimize risks and allocate risk associated with the other company in such a manner that it would lead to maximization of shareholder value. This process involves exchange of documents between the companies and reviewing them. Based on the documents, a data room is set up and a requisition list is created. Once the documents are reviewed and risks are identified, the target company is consulted to understand the risks. If the risks are explained adequately, then they are dismissed. If not, then depending on the risk, the shareholder is

protected through conditions precedent or subsequent, representation and warranties. Reviewing the documents, a report consisting of different chapters would be made, outlining each of the fundamental aspects which are scrutinized. These chapters ordinarily would be corporate secretarial, property, debt, litigation, permits and licenses, substantial agreements, and employees.

After the identification of risks, there is the drafting and negotiating process where companies or persons ask for rights for their own protection. First, there is the process of negotiation where parties ask for rights associated with the company. These include veto rights, board rights, information rights, anti-dilution rights, pre-emptive rights, exit rights, representations, and warranties. Along with these, there are also boilerplate clauses and liquidation preferences of shareholders. Each of these rights have a strategic significance geared towards control, exit or prospective stake in the company. All of these must be outlined in a definitive document, those being the shareholders' agreement and the share purchase or share subscription agreement depending on the nature of the deal.[4]

Once the rights have been negotiated and definitive documents are drafted, the company then passes a shareholders' resolution to signify that the existing shareholders are not against the negotiated terms. After the same, an offer letter is circulated detailing the price of the shares, number of shares and other terms to the prospective acquirer. Once the incoming shareholder accepts, the share subscription or purchase agreement leading to the transaction gets executed. Before everything to the effect of the negotiation is put into effect, it must also be shown that the conditions before the closing of the deal are satisfied. These are conditions precedent, identified in the due diligence and negotiated between the parties, without which the parties do not accept other terms. On the other hand, there might also be conditions subsequent which are conditions that need to be completed after the deal has taken place. These are typically obligations that can be even fulfilled at a later point because of their unhurried nature. Once the conditions precedent are satisfied, the placement process is closed. At closing, it is ensured that the application has been accepted, the payment for shares has been completed, issue of share certificate is done and

[4] "Matthew Shakesheff, '*How to prepare for a share acquisition: your legal guide*' (HARPER JAMES, 16 February 2023) https://harperjames.co.uk/article/how-to-prepare-for-a-share-acquisition/" last visited 18 August 2023.

register of shareholders has been updated, board resolution has been passed and the registrar of the companies has been updated.

III. Key Considerations in Due Diligence of Technology Companies

In an acquisition in technology companies, the process of private placement follows the same series of steps as another traditional company. However, there are certain key considerations, which change for technology companies. As discussed, the due diligence process that is followed for traditional companies at the present approach lays heavy focus on corporate secretarial, financial indebtedness, property, employees, agreements, licenses, and litigation.[5] While these considerations are important even in a due diligence report for technology companies, there are some identifiable areas that need to be given special attention. The areas that have been identified by the author are as follows:

1. Intellectual Property
2. Licenses relating to the technology
3. Veracity of the technology (compliances with the standards)
4. Standard of cyber security to be maintained
5. Maintenance of servers
6. Employees
7. Data production, identification, and localization
8. International Compliances

These areas jointly analyze the essence of technology companies. It is what basically differentiates tech companies from traditional companies. Some of the analysis in the paper may be hypothetical in nature, but overall, all these pieces come together to form a perfect whole. This paper will attempt to go into the details of each category and analyze how a Transactional lawyer can tackle them to render a more effective service to a client.

1. Intellectual Property

[5] "Churu Mathur, '*India: Legal Due Diligence*' (MONDAQ, 30 July 2002) https://www.mondaq.com/india/operational-performance-management/17241/legal-due-diligence" last visited 17 August 2023.

Starting off, as such, intellectual property is already stressed in due diligence of traditional companies. Lawyers make sure that the trademarks and patents over the products offered by the parties are valid. Sometimes, the status of the same may appear disputed. In such cases, it becomes the duty of the lawyers to flag the risks associated with disputed patents or trademarks. Trademarks create an identity for the company when it distinguishes the products of a company with the products of other companies. If the trademark registrations are not in order, then the parties may only be able to claim limited protection from the law, which might dissuade a potential acquirer, especially when the brand name of a company is a focal point.

On the other hand, patents are exclusive rights for an invention that is either a product or a process. The product generally provides a new way of doing something or a new technical solution to a problem. In Indian law, the essentials for a patent are that it must not be a non-patentable subject, have novelty, have industrial application, and is an inventive step. For a patent to be granted, it needs to be first published and disclosed to the public. For technology companies, patents might become very important. It has been stated that the current patent laws prescribe a set of general rules to govern the validity and infringement of patents in a wide variety of technology[6]. A lot of new age companies pride themselves over the state-of-the-art technology.[7] These companies need patents associated with the required technologies to seem appealing to the investors. If the same is not done, then practically, any other company can utilize the technology for their own gains. This would ultimately result in the company with the initial idea to lose out on any advantage accrued from the technology. Further, if the patent is filed by another company, then the company could be liable to compensate for the unauthorized use of patents. Further, it is also required to investigate the patent approval.

Lastly, even copyright has a role to play in a legal due diligence concerning technology companies. Under Section 2(o) of the Copyright Act, "literary work" includes "computer programs, tables and compilations including computer databases." Therefore, computer programs are under the ambit of being protected.[8] In technology companies, some codes may be of important value and the creators in the company might not want the code to be utilized by

[6] "Dan Burk and Mark Lemley, *Is Patent Law Technology – Specific*?, 17, BERKELEY TECHNOLOGY LAW JOURNAL (2002) .

[7] "Nat Watkins, '*Inside Big Tech's Race to Patent Everything*' (WIRED, March 15, 2022) https://www.wired.com/story/big-tech-patent-intellectual-property/ last visited 18 August 2023.

[8] "The Copyright Act, 1957 , 14 of 1957 (India).

other professionals in other companies. Hence, copyright protection is awarded. As such, a work becomes copyrighted as soon as it is published. Given the same, it might be a good practice to preserve evidence of its publication. That way, rights relating to the work can be exercised by people

2. Licenses relating to the technology

Licenses relating to a technology can come into consideration in two major ways. Firstly, a company that has been granted a patent may grant a license to other companies for a consideration under patent law.[9] Usually, such license is granted for some consideration. An agreement for a license would need to be reviewed by investors to make sure how other companies utilize the same technology and for what period. If the license is granted to multiple companies, then the company granting the license may have increased the competition for itself in interest of compensation from other companies. In this aspect, the term of the license and the extent of usage would need to be seen. It would need to ensure that the other companies have not been granted the option to sub-license the technology. Otherwise, that would lead to quick saturation in the market. Even the purpose of granting the license would become a factor.

Furthermore, if a company is utilizing a license granted for another company, these considerations talked about above become important again. The main considerations for the licensee company become the term of the license, the consideration which the company provides and the purpose of the issue. If the license has been granted, but if the technology cannot be used for commercial purpose, then it would essentially be useless, unless the company is a research based one. Further, it would not make sense for the investor to invest if the company is hemorrhaging money by paying a hefty fee for the license. Lastly, if there are no terms for renewal in the existing contract or if the terms must be renegotiated again at the expiry of the license or if the license is granted for a very short period, the future of the company can become uncertain when the company bases its primary operations on those licenses.

3. Veracity of the Technology

[9] "Sonal Sodhani, '*India: Patent Licensing*' (MONDAQ, May 15, 2019) https://www.mondaq.com/india/patent/805902/patent-licensing" last visited 19 August 2023.

A lot of private companies that receive investment or get acquired, face such situations in their initial growth stage; therefore, all their operations at the time may not have been successfully established. In such cases, investors need to make sure that the technology, the company is based on is genuine. It needs to be ascertained if the company's technology can be scaled and can be used to generate sustainable profits. Although, lawyers may not be competent to comment on the exact working of the technology or verify if it works correctly, their job can extend towards investigating the data produced by the technology, assessing the business model surrounding the piece of technology and check if the policies of the company have been framed accordingly. Accordingly, checking for any additional requirements by the government surrounding a new technology is always a good idea.

4. Standards of Cyber Security

In the long run, it needs ensured that the company using the technology has taken adequate safety measures to ensure that harm is not caused to any stakeholders associated with the company. It is essential that required standards by the law at the very least should be met by the company. Some reasonable security practices and procedures have been given in "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011" ("**SPDI Rules**").[10] These rules were brought into force through exercise of powers conferred by clause (ob) of subsection (2) of Section 87 read with section 43A of the Information Technology Act, 2000. Rule 8 prescribes certain reasonable security practices and procedures. It states that "a body corporate would be said to have complied with such practices and procedures in the case they have implemented such practices and have comprehensive documented information security program and information security measures that are commensurate with the information assets being protected with the nature of the business." As a reference of the standards, the Rule lays focus on IS/ISO/IEC 27001 on "Informational Technology – Standard Techniques – Information Management System – Requirements". As per Rule 9(3), in case the entity wants to follow practice other than the ones prescribed by IS/ISO/IEC, then such practices need to be approved and notified by Central Government. Even though, other practices can be adopted, it is to be noted that ISO/IEC 27001

[10] "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf"

has been the international standard for informational security. Along with the protection of data kept by companies, it results in an organization's resilience towards cyber-attacks and reduction of information security costs.

However, it should be noted that the stated Rules were brought into effect in 2011. Much time has passed since then, and technology has changed. At the time of writing this paper, the Digital Personal Data Protection Bill, 2022 ("**DPDP Bill**") has been released in form of a draft.[11] This bill is expected to remove the requirements that were brought by the previous rules through the application of Section 30(a), which would omit Section 43A of the Information Technology Act, 2000 in its entirety. Therefore, the standard set by the Rule would go away too. However, the draft bill has certain provisions of its own concerning safety standards. Section 9 which deals with the general obligations of data fiduciaries in its sub-section (4) lists that data fiduciary and data processor shall protect personal data in its possession or under its control by taking reasonable security standards to prevent personal data breach. Further, Item 1 in Schedule 1 prescribes a penalty upto 250 crores for non-compliance of Section 9(4). While the angle of penalty is novel and might prove quite effective, the draft Bill does nothing to state what 'reasonable security standards' would mean. Even though, the penalty itself may act as a huge deterrent for companies to take proper precautions, smaller companies can prescribe to lower standards in case they deem it 'reasonable'. The word has the capacity to be interpreted differently by different parties. Therefore, a clearer minimum standard may have been more suitable.

It is to be also noted that Section 9(4) of the DPDP is geared towards protection of personal data only. However, it prescribes no requirements for cybersecurity, which constitutes a larger discipline also incorporating privacy and may be essential for the company to survive.[12] The previous IS/ISO/IEC standard was geared towards informational security as a whole and therefore, was comprehensive. The current wording of the provision could be problematic. Even so, since it is upon the companies to make sure that their stakeholders are not harmed, due

[11] "The Data Protection Bill, 2022 (India) https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf" last visited 17 August 2023

[12] "Mark R. Heckman, '*The Difference between Data Security and Privacy*' (UNITED STATES CYBER SECURITY MAGAZINE, Winter 2017 Issue) https://www.uscybersecurity.net/csmag/data-security-privacy/" last visited 23 august 2023.

diligence reports should ensure that the companies have prescribed to proper cybersecurity standards and the certification of the same must be given to the clients. Each operating industry can have a different cybersecurity standard, therefore, the same should be checked upon.[13]

5. Maintenance of Servers

Server technology refers to the type of the computers that manage and provide access to specific resources for other devices and users. These are typically located within a business for the management of access to files, web content, multimedia content, email, retail messaging and other functions.[14] Due to the importance of servers in a technology company, it needs to be investigated if servers are adequately maintained in the company and if there are any problems that can be caused in the future. One of the standards that may apply to physical servers of a company are Fire Protection of Electronic Data Processing Installation – Code of Practice, which was adopted by the Bureau of Indian Standards.[15] Even though laws in India may not provide for comprehensive standards for the protection of company standards, it is always a good idea to make sure that the company has taken adequate protection, especially in technology companies. And even though acquiring non-mandated high protection may incur a cost, the overall objective of making the company more secure is satisfied. It would make the company more valuable due to the protection offered to its own assets and data of other people. In furtherance of the same, some standards that can be looked at are provided by National Institute of Standards and Technology in the US in the publication titled "Guide to General Server Security".[16]

In line with the discussion around servers, the Indian Computer Emergency Response Team ("**CERT-In**") on April 28th, 2022, had issued a set of directions involving information security practices, procedures, prevention, and reporting of cyber incidents for establishing a safe and

[13] "AAT Team, '*Complete List of Cyber Security Standards*' (AAT, January 4, 2023) https://allabouttesting.org/complete-list-of-cyber-security-standards/" last visited 18 August 2023.

[14] "Dell Technologies, '*Server Technology*' (DELL) https://www.dell.com/en-in/work/lp/server-technology#:~:text=Server%20technology%20refers%20to%20types,backups%2C%20applications%2C%20and%20more." Last visited 20 August 2023

[15] "Indian Standard Fire Protection of Electronic Data Processing Installation – Code of Practice (*Bureau of Indian Standards*, September 2004) https://law.resource.org/pub/in/bis/S03/is.12456.2004.pdf" last visited 23 August 2023.

[16] "Karen Scarfone, Wayne Jansen and Miles Tracy, '*Guide to General Server Scrutiny*' (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, July 2008) https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf" last visited 24 August 2023.

trusted environment on the internet.[17] The requirements provided under these directions extend to intermediaries, service providers, data centers, virtual asset service providers and virtual asset exchange providers. Barring those requirements specifically associated with virtual private networks, the directions provide for mandatory reporting of cyber security incidents, compliance with directions given by CERT-IN, synchronization of ICT systems clocks to NTP Server, enabling logs of all their ICT systems and maintaining them for 180 days in the Indian jurisdiction for all other entities covered under these directions. If applicable to a particular company that may be covered above, a company must showcase that these requirements are met, specifically relating to their servers.

6. Employees

One of the most valuable assets in technology companies become their employees.[18] A technology company can have multiple employees where only certain employees may be at a sophisticated level to understand the works that are being engaged in. Of course, employees at a lower level can usually be replaced and trained from the very scratch. However, as employees go up the ladder, companies do not have the ability to replicate the skills of the employees at a higher level. In such cases, it becomes essential for companies to preserve their talent and offer them opportunities to make sure they don't leave the company. From a legal point of view, the work culture of a company and the motivations of the employees cannot be accurately measured. Even so, a potential investor in a company must ensure on their part that the future of company in terms of talent options is secured.

A method of ascertaining the term of employees in the company is seeing their employment contracts. If they are employees engaged in key operational roles, the company would want to secure them. Hence, the term of the contracts could be for a longer period. If the renewal of employee contracts is for a longer amount of time, it would mean that employees see themselves associated with the company for a long time. On the other hand, necessary provisions must exist in the contract where the terms of employment or employee can be changed depending on the

[17] "Nishith Desai, '*Cyber Security: India revamps rules on mandatory incident reporting and allied compliances*' (NISHITH DESAI, May 06, 2022) https://www.nishithdesai.com/generateHTML/5507/4" last visited 24 August 2024.
[18] "William Vanderbloemen, '*This is Why People (Not Technology) are still your greatest Asset*' (FORBES, December 8, 2016) https://www.forbes.com/sites/williamvanderbloemen/2016/12/08/this-is-why-people-not-technology-are-still-your-greatest-asset/?sh=74aebd68640d"

situation. These contracts, while not being publicly available can be provided by the private companies at the instance of the investors.

Another method to ensure that employees stay onboard could be the issue of Employee Stock Option Scheme. As such, if employees have a stake in the company, then they are motivated to make sure that the company does well. Therefore, if an employee receives ESOPs that could vest and be exercised over longer periods, then they have an incentive to stay in the company. An ESOP scheme can be easily assessed by seeing the documents that a company files with the Ministry of Corporate Affairs. Generally, they are present in the Articles of Association. If the same is not the case, then MGT-14 filings can be accessed to make sure ESOP schemes have been passed.

7. Data production, identification, and localization

A technology company is bound to process data. In fact, all companies produce and process data. It's just that technology companies tend to deal with higher amounts of data due to big data algorithms and then using data to provide service to users. Therefore, technology companies need to be more careful when dealing with the legal framework around data.

Firstly, it needs to be ascertained what kind of data the company makes use of. If the type of data is personal, then there are specific legislations and rules that come into play to make sure that data of consumers are protected. In this context, the SPDI rules and the DPDP Bill become particularly important.

The SPDI Rules provides for what is personal information in the Indian context. Rule 2(i) states that personal data is *"any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person."* Further, the Rules also provide as to what sensitive personal data is. Rule 3 includes passwords, financial information, health conditions, sexual orientation, medical records, biometric identification, and any related data received by body corporate or processed by them. Therefore, both rules provide as to what sensitive or non-sensitive personal data would consist of. Any data that does not fall under these categories can be considered as non-personal data, which is not governed in India.

On the other hand, the current iteration of the DPDP Bill, 2022 which is set to replace the SPDI Rules in the future has similar provisions to it. For instance, Section 2(13) describes personal data as "any data about an individual who is identifiable by or in relation to such data". In principle, both definitions of personal data seem to have the same effect. Both tender towards pseudonymization, identifiability and relation to data.

From a technology company's perspective, once they identify that they make use of personal data, they need to make sure that processing happens in accordance with the provisions of the Rules or the Bill, whichever seems to be in force at the time. As such, the previous SPDI Rules did not provide for any penalties explicitly. Recently, the same has become more important for a company because of the penalty provided for the DPDP Bill. Schedule 1 in consonance with Section 25 provides that any other non-compliance with the Act that those specifically listed in the Schedule has a penalty up to 50 crores. Further, the other penalties provided in this Act extend to 250 crores. For a new technology company, which has no option, but to comply due to the nature of the work, this constitutes a lot of money. Any fee under the Act has the capacity to cause huge losses and hence, put the investors at risk. It only makes sense for an acquirer to check compliance before investing.

A lot of these technology companies may have their servers outside the country, especially if they provide services outside India or are based in other countries. On the other hand, when mergers happen, data regarding consumers or previous processes also become transferable elements. For the same, the transfer of data is currently governed by the SPDI Rules and of course, the DPDP will govern it in the future. As per Rule 7 of the SPDI Rules, transfer is not problematic. It states that a body corporate can transfer data to another body corporate outside or within India provided the transferee has the same level of data protection that is adhered by the transferor under these Rules. However, transfer may only be allowed for the necessity in performance of lawful contract between the transferor and provider of information or where the data subject has consented to such transfer. In M & A, between the companies, due to this Rule, companies may run into a problem where the consent of its employees are necessary for transfer of data. And while employees may give their consent, the process is highly inefficient and takes a lot of time. Lately, this has become a problem.

This problem has been attempted to be solved by the DPDP Bill. Under Section 8(8)(b), deemed consent is said to be given in public interest including mergers, acquisitions, or any other similar combinations or corporate structuring transactions in accordance with the provisions of applicable laws. Due to the provision of deemed consent, consent would have been said to be given in any transaction involving corporate structuring. Therefore, this provision has been directly included to fight any setback that comes in these transactions because of employees not providing their consent. Further, the provision seems large enough to subsume the consent of consumers within the purview of mergers and acquisitions. Lastly, companies should make an endeavor to localize their data due to Section 17 stating that only the Central Government can notify such countries or territories outside India to which a Data Fiduciary may transfer personal data. Therefore, it is not clear as to where the data can be transferred. It is also unclear if Section 8(8)(b) subsumes Section 17.

8. International Compliances

Due to shrinking international boundaries of operation, technology has the capacity to affect people globally rather than just in the country. For instance, a company in India might want to offer their services abroad. Considering such cases, laws across the globe have been shaped in such a manner that technology companies need to meet compliances in other jurisdictions for them to set up their operations in a particular country. A good example of this would be the General Data Protection Regulations ("**GDPR**").

The GDPR, as such, is considered as the benchmark for data governance.[19] Regulations that might be adopted across the globe are expected to have similar provisions to that of the GDPR, including India's DPDP Bill.[20] Under Article 3 of GDPR, the regulations apply to "processing of personal data of data subjects who are in the European Union ("**EU**") where the processing of data is linked with offering of goods or services or monitoring of the behavior of data subjects as

[19] "Mitch N, '*A Benchmark for Data Protection Regulations: GDPR and PIPA*' (LINKEDIN, November 10, 2021) https://www.linkedin.com/pulse/benchmark-data-protection-regulations-gdpr-pipa-mitch-no/" last visited 20 August 2023.

[20] "Thales Group, '*Beyond GDPR: Data Protection Around the World*' (THALES, 10 May 2021) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world" last visited 16 August 2023.

far as their behavior takes place within the EU."[21] Article 3(2) also states that such provisions apply to processing by a controller or processing not established in the European Union. Therefore, while the GDPR is adopted only in the EU, its compliances stretch globally.

Due to the wide territorial scope of data governance laws around the globe, if a technology company offers its services globally and deals in processing of personal data (which they will in all probability), they will have to comply with regulations pertaining to each country. While there are similar provisions that might be outlined in every legislation, each country or region is bound to have some degree of varying laws.

Further, another consideration might also be the kind of laws that are likely to impact the company in the future if they do decide to operate internationally. For instance, if a company engages in the usage or creation of Artificial Intelligence ("**AI**") systems, the compliances required in India might be minimum and limited to the latest data processing law. However, there is a pending AI Act proposal in the EU.[22] The proposal has the capacity to become a law and necessitate higher compliances to AI systems operating in the EU or affecting EU markets. When the company goes international, the law will impact the company.

Therefore, two considerations arise in due diligence with regards to what has been mentioned above. They are the vision of the company and the expected market of the product or service offered by the Company. Firstly, given companies might be in the growth stage when Venture Capitalists or Private Equity investors come in, a vision of the company would need to be reviewed before investing. If the company eventually wants to offer its services internationally, then lawyers need to make sure that the company is future proof. Secondly, the investors would need to review scalability considering differing legislations. If a company is only profitable if its user base stretches globally, then compliance with laws would be necessary. And compliances bring about additional costs, which the investors will need to factor in when making the investment. For instance, the costs under the AI Act for compliance with a high-risk AI system

[21] "General Data Protection Regulation, 2016/679, Article 3, (2018) https://gdpr-info.eu/art-3-gdpr/"lasted visited 17 August 2023.
[22] "Future of Life Institute, '*The AI Act*' https://artificialintelligenceact.eu/"

might be very high.[23] Therefore, an investor needs to consider costs when the business would expand.

IV. Deal Structuring

As such, due to the factors above, a lot would not change when it comes to how the deal is structured. Of course, an investor may typically ask for a board seat and an observer right to see how the board has been functioning and what their decisions are. But being fair, these rights are granted in any acquisition or merger.

On the other hand, an investor or an acquirer cannot ignore any issues or red flags that come out of a due diligence. They need to be addressed. For the same purpose, when the parties enter the negotiation stage and discuss the rights that will be traded, there need to be discussions around representations, warranties and indemnifications directly accruing from the risks in the due diligence. As such, a representation is a fact that is relied on by the receiving party to enter a contract. Therefore, they can be described as statements which a party affirms to be the truth. On the other hand, a warranty is a promise that a condition or assertion is true and if the same does not amount to the truth, parties usually provide each other with promise of indemnity. The distinction between a representation and a warranty typically is that the former accrues to the facts on the present day while the latter focuses on conditions that may come into play in the future.[24]

In technology companies, the warranties and the representations that are to be given by the company directly correlates to each of the seven situations discussed, in addition to other issues found by the due diligence. As such, issues relating to intellectual property can be usually recognized by a due diligence and can easily be solved by conditions precedent before the deal closes. Of course, if the patent related to the company is not granted, then a clause for warranty protecting the share value or damages can be initiated in the Shareholder's agreement as that would be something fundamental to the company. The investor is bound to face loss without a

[23] "Benjamin Mueller, '*How much will Artificial Intelligence Act Cost Europe?*' (INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, July 26, 2021) https://itif.org/publications/2021/07/26/how-much-will-artificial-intelligence-act-cost-europe/"

[24] "Ashima Obhan and Vrinda Patodia, '*India: Revisiting Representation and Warranty Clauses*' (MONDAQ, 19 June 2020) https://www.mondaq.com/india/contracts-and-commercial-law/955660/revisiting-representation-and-warranty-clauses"

warranty in that scenario. On the other hand, if the company states that there has been no sub-license of their technology, then a representation on that basis must be undertaken in the shareholder's agreement entered between the parties. Or a warranty can be undertaken accruing to the renewal of license contract.

For the other factors, usually, these issues can be solved again through conditions precent or subsequent. For instance, the investor can put a condition precedent in the agreement that the company needs to maintain certain cyber security standards or standards for the servers. Ascertaining a situation where the same is not done, the parties can negotiate a warranty or representation clause. For key employees, logically, the company cannot make sure if they would stay. They can provide incentives but that may not ensure the term of employees either. In such circumstances, the investor on an acquirer can enter a clause stating that the company would make its best efforts to ensure that the employees do not exit the company.

Lastly, relating to data protection and localization, a representation clause should typically assure the investor of what the company is doing and planning to do.

V. Conclusion

Through the seven factors discussed in the paper, the paper attempts to create a scenario where a lawyer could do proper service to their client in a matter of due diligence and deal structuring. While these factors have been arrived at, they may not be exhaustive or even applicable in each scenario. As such, it cannot go unnoticed that each company, even a technology company, might be different at its core. Some technology companies might derive their value from their underlying patent, while some might be a healthy investment due to their consumer base. Other technology companies might provide good service due to their excellent employees. The point is that there is a lot of variation and specialized due diligence must be done for each company to arrive at the risks. Even so, these seven factors provide a good starting point, at least, in theory.

Moreover, the company may not grant all the rights asked for associated with the risks. In the end, if an investor wants heavy returns on their investment, they must be willing to take some risk. The promoters of the company cannot practically manage to protect only their investors and not the company. Therefore, the rights can be asked for a negotiation, but they must be observed with a grain of salt.

Lastly, if the premise is that all companies are going to be technology companies in the future, it stands to reason that all lawyers must evolve. Lawyers cannot afford any longer to be only involved in corporate or securities of a company. If that happens, a lawyer specializing in security or corporate and technology laws will dominate. Therefore, corporate lawyers of tomorrow also need to be technology lawyers. At the very least, they need to be aware of the basis data protection or cyber security law that may come into force tomorrow. As the author of the paper sees it, it is only a matter of time before technology becomes all pervasive.

SAFEGUARDING FINANCIAL INCLUSION: DEVELOPING A REGULATORY FRAMEWORK FOR BUY NOW PAY LATER SERVICES IN INDIA

- *Harshit Chauhan &Dhrutvi Modi*[1]

Abstract

The global lending ecosystem is undergoing a profound transformation, with digital platforms for Buy Now Pay Later (BNPL) products witnessing significant expansion. Established fintech firms, e-commerce giants, and tech corporations have entered the BNPL space, attracting substantial investments and reshaping consumer finance. India's BNPL sector, in particular, has experienced remarkable growth, outpacing the year-on-year growth of the Unified Payments Interface (UPI). However, the Reserve Bank of India (RBI) issued a directive in June 2022 that prohibited non-bank prepaid wallets and prepaid cards from providing credit lines to BNPL platforms, causing disruptions in the industry. This article analyses the issues surrounding the BNPL industry in India, delving into market penetration, the RBI's regulatory decision, and its implications. It also explores the regulatory frameworks for BNPL in Australia, Denmark, and Hong Kong, offering a comparative analysis of their approaches. In India, BNPL services have witnessed exponential growth, driven by factors like efficient online lending processes, quick disbursal of funds, and increased demand for repeat loans. However, the RBI's directive to discontinue loading PPIs via credit lines has raised concerns about its impact on financial inclusion and credit accessibility for underserved populations. Australia has taken a balanced approach to regulate BNPL, requiring providers to hold an Australian credit license while maintaining a flexible regulatory framework. This approach aims to ensure responsible lending practices while allowing the industry to thrive. Denmark's regulatory framework focuses on consumer protection, mandating BNPL companies to obtain a consumer lending license, conduct creditworthiness assessments, and align products with target audience needs. The amendments

[1] 4th Year, Gujarat National Law University. Gmail: harshit20bal030@gnlu.ac.in&dhrutvi20bal054@gnlu.ac.in

narrow exemptions for BNPL products, reducing the risk of consumers falling into debt traps. Hong Kong has adopted a moderate approach, with the Hong Kong Monetary Authority (HKMA) issuing a circular to enhance consumer protection for BNPL products. While Hong Kong's regulations are evolving, they currently apply to banks and licensed money lenders, leaving a regulatory gap for other types of institutions. In summary, India's regulatory approach is cautious and comprehensive, while Australia strikes a balance between regulation and industry growth. Denmark emphasizes consumer protection, and Hong Kong's approach is evolving. The comparative analysis highlights the diverse regulatory strategies employed to address the challenges associated with BNPL services, reflecting each country's unique regulatory landscape and priorities. Balancing consumer protection with financial inclusion remains a key challenge across all jurisdictions.

Keywords: *BNPL, Financial Inclusion, Digital Lending, FinTech, Financial Regulator*

I. Introduction

The lending ecosystem is going through a paradigm shift and the use of digital platforms for Buy Now Pay Later (BNPL) products has expanded markedly. The increasing adoption of BNPL solutions and the accomplishments of established FinTech firms in this field are motivating the entry and funding of fresh participants. Despite being relatively new, the competition in the market for BNPL services is growing more intensely. This industry has attracted significant investments on a global scale, leading to the success of start-ups and even well-established FinTech companies like PayPal and Paytm, e-commerce platforms such as Amazon (Amazon Pay Later) and Flipkart (Flipkart Pay Later), and major technology corporations like Apple (Apple Pay Later) have ventured into the BNPL domain by offering their own solutions. Many financial institutions and stakeholders are acknowledging the potential of BNPL and its capacity to transform consumer finance.

Over the past few years, the BNPL sector in India has also experienced remarkable growth, emerging as one of the fastest-growing industries in the country. With an exponential growth rate of 569% in 2020 and a staggering 637% in 2021. The growth rate of the BNPL industry in India had outpaced the year-on-year growth of UPI, which was recorded at 174%.[2] However, on June 20th, 2022, the Reserve Bank of India (RBI) issued a direction that had a profound impact on the entire BNPL industry. This notification prohibited non-bank prepaid wallets and prepaid cards from providing credit lines to these platforms. Paragraph 7.5 of the Master Directions on Prepaid Payment Instrument (PPI), specified that PPIs could be loaded and reloaded with cash, debits from bank accounts, and credit or debit cards. Consequently, it implied that loading PPIs via credit lines, loans, or advances is not permitted.[3]

To put it simply, this decision delivered a significant setback to some of the rapidly expanding Indian fintech start-ups. These start-ups, with their credit lines, have played a crucial role in advancing financial inclusion and digitalization in India. Consequently, the given article aims to analyse the issues associated with the BNPL industry in India. The second section aims to discuss the demand and market penetration of BNPL products in India. The third part gives an

[2] Sindhu Hariharan, 'Buy-now-pay-later grows 600%, overtakes UPI payments' *The Times of India* (Chennai, 01 February 2022) https://timesofindia.indiatimes.com/business/india-business/buy-now-pay-later-grows-600-overtakes-upi-payments/articleshow/89256906.cms accessed 19th July 2023

[3] Reserve Bank of India, *Master Directions on Prepaid Payment Instruments (PPIs)* (RBI/DPSS/2021-22/82)

insight on why the RBI is imposing regulations that impede its growth and its implications. The fourth section aims to highlight regulation of BNPL in other jurisdictions. The fifth section aims to draw a comparative analysis of the regulatory framework of BNPL. Lastly, the sixth section provides a way forward.

II. Market Penetration in India

While exploring the macro perspective of micro financing, it is observed from the credit ecosystem trends in India[4] that the markets in the metro cities and large format retail stores have already been presented with solutions by traditional large lenders, including banks and non-banking financial companies (NBFCs), have a strong urban focus when it comes to retail loans. Approximately half of the loans they extend are concentrated in just eight major cities categorized as Tier-1 accounted for 46.5% of the total origination balances and 39.3% of the total origination volumes in 2018[5]. Among all the financial products, credit cards exhibit the highest level of concentration, with Tier-1 cities contributing to approximately three-fourths of the total aggregate. These urban centres play a significant role in driving the retail loan market in the country. As a result, the scalability and volume of low-ticket price lending products is low.

This is not the same in Tier-II and beyond than just the metros, which have witnessed high volume of low-ticket price lending products. This is because Tier-II cities and beyond often have a larger untapped market for credit services, as the level of financial inclusion and access to formal credit sources is typically lower in these areas compared to metros. Additionally, there may be more small and medium-sized enterprises (SMEs) in these areas that need credit services. Several other factors have contributed for the growth of BNPL products such as faster and efficient online lending process, taking only a few minutes to register, upload documents, and apply for a loan. Disbursal of funds is also instant, making borrowing convenient, especially during emergencies. The ease of borrowing leads to increased demand for repeat loans, and

[4] Experian-Invest India, 'A Review of India's Credit Ecosystem' (2021).
[5] Gayatri Nayak, 'Eight top tier-I cities together account for almost half of retail loans' *The Economic Times* (24th September 2018) < https://m.economictimes.com/news/economy/finance/eight-top-tier-i-cities-together-account-for-almost-half-of-retail-loans-in-the-country/articleshow/65938533.cms > accessed 24th July 2022

lenders benefit from improved loan management through AI, social media verification, and data analytics[6].

In Q4 of 2022, there was a substantial surge in demand for BNPL services, with LazyPay, ZestMoney, and KreditBee being some of the prominent providers experiencing this trend.[7] However, it is important to note that the size of the opportunity can differ within and beyond a specific region and market conditions. Distribution and affordability are important for consumer acquisition on conversion into customers for small merchants, which when plugged-in as a financial service and assists in underwriting of borrowers. Small merchants contribute 80% to India's retail[8], however consumers are devoid of access to merchant network and remain unpenetrated at a category specific level. Therefore, the BNPL products offered by fintechs create a large distribution network in smaller towns and generating incremental transaction, which was not available in the consumer finance space, thereby increasing the efficiency of the market.

III. Reasons and Implications of prohibiting loading of PPIs via Credit lines

A significant number of the PPI operators offer BNPL services, predetermined borrowing limits or credit lines that enable customers to access credit within the specified limit as needed. In this context a 'credit line' can be understood as a type of virtual credit that doesn't involve an immediate transfer of the borrowed amount to the recipient's account. Rather, as a flexible credit arrangement, providing access to funds whenever they are needed on demand. Therefore, these services are like short-term loans that incur interest on default, but they come with a deferred payment period. The RBI in its June 20, 2022, directive to the authorized non-bank PPI issuers stated that **loading PPIs** from **credit lines** is **not allowed**, and any existing practices of doing so

[6] Rohit Garg, 'Why are small-ticket loans gaining popularity in today's environment? Here are the reasons' *The Times of India* (03rd April 2022) < https://timesofindia.indiatimes.com/blogs/voices/why-are-small-ticket-loans-gaining-popularity-in-todays-environment-here-are-the-reasons/ > accessed 24th July 2022

[7] Research and Market, 'India Buy Now Pay Later Business and Investment Opportunities Databook - 75+ KPIs on BNPL Market Size, End-Use Sectors, Market Share, Product Analysis, Business Model, Demographics - Q2 2023 Update' (2023).

[8] FE Online, 'Over 30,000 small, medium brands in retail catering to 80% of India's population: CAIT' *Financial Express* <https://www.financialexpress.com/industry/sme/msme-eodb-over-30000-small-medium-brands-in-retail-catering-to-80-of-indias-population-cait/2494199/ > accessed 27th July 2022

must be immediately discontinued. This directive aligns with the RBI's Master Directions on Prepaid Payment Instruments (MD-PPIs), as notified on August 27, 2021[9].

The Regulations outlined in the MD-PPIs are applicable to both PPI Issuers and System Participants. While PPIs can be issued by both banks and non-banks, this requires obtaining prior approval or authorisation from the RBI. Thus, establishing, and operating payment systems for PPIs requires authorisation under the Payment and Settlement Systems Act, 2007.[10] Due to the absence of clear guidelines, companies were able to exploit a grey area, taking advantage of the lack of specific regulations or rules. Non-bank PPI issuers, which could not launch a credit line and even fintech companies with no PPI or NBFC licence partnered with banks or entered co-branding arrangements to provide credit lines, while others obtained funds from NBFCs.

For instance, Garagepreneurs Internet Private Limited ("Slice") holds a PPI license[11] and issues co-branded PPI card "slice Card"[12] functioning as a stored value account issued by SBM (State Bank of Mauritius) under a co-branding agreement with Slice, which acts as the co-branding partner.[13]At the same time it functions as a digital lending platform or loan facilitator on behalf of its financing partners (NBFCs) like Quadrillion Finance Private Limited, DMI Finance Private Limited, and Northern Arc Capital Limited, etc[14] which provide credit line to their product. A similar model of providing a credit line is common amongst several companies such as Uniorbit Technologies Private Limited – Uni Card, FPL Technologies Private Limited – One Card, etc. As a result, the directive against the loading of PPIs via credit lines posed a direct challenge for the companies offering BNPL services and this is where the core contention of the fintech players arises.

[9] ibid 2.
[10] Reserve Bank of India, *Certificates of Authorisation issued by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for Setting up and Operating Payment System in India*(RBI 2023).
[11] Tarush Bhalla &Digbijay Mishra, 'Card fintech company Slice receives prepaid pay licence from RBI' *The Economic Times* https://economictimes.indiatimes.com/tech/startups/card-fintech-company-slice-receives-prepaid-pay-licence-from-rbi/articleshow/96260168.cms?from=mdr accessed 07th August 2023
[12] Slice, 'TERMS AND CONDITIONs' (*sliceit.com)* https://www.sliceit.com/T&C/ accessed 07th August 2023
[13] Slice, 'Our banking partners' (*sliceit.com)* < https://www.sliceit.com/banking-partners/ > accessed 07th August 2023
[14] Slice, 'Our financing partners' (*sliceit.com)* < https://www.sliceit.com/financing-partners/ >accessed 07th August 2023

The RBI directive came with a three-pronged objective:

i. Firstly, to establish a comprehensive framework that outlines the process for granting authorization, regulating, and overseeing entities involved in issuing and operating PPIs within the country. This framework ensures that the operations of these entities are well-monitored and compliant with the necessary regulations.

ii. Secondly, to encourage healthy competition and promoting innovation in the PPI sector in a responsible and cautious manner. While doing so, special attention is given to the safety and security aspects of the payment systems and transactions, as well as safeguarding the interests of customers and ensuring their convenience.

iii. Lastly, to facilitate the harmonization and interoperability of various PPIs. This means creating a system where different PPIs can seamlessly work together and be compatible with one another. By doing so, it enhances the overall efficiency and ease of using prepaid payment instruments, benefiting both consumers and businesses alike.

Consequently, the RBI's directive, centered on safeguarding customer well-being and reducing cybersecurity vulnerabilities, primarily focuses on addressing the issues associated with app-based PPI operators that provide indirect credit facilities. These difficulties include concealed expenses, insufficient assessments of affordability, inconsistent regulatory criteria, and deficiencies in financial knowledge. Conventional financial institutions must adhere to stringent capital adequacy and KYC requirements when granting loans.

However, the lack of standardized KYC and underwriting procedures among PPI operators has led the RBI to establish more uniform guidelines. Moreover, the Working Group on Digital Lending through Online Platforms and Mobile Apps constituted by RBI in 2021[15] had a clear objective to strike a careful balance between fostering innovation and ensuring safety within the digital lending sphere. A strong emphasis was laid on the obligatory enforcement of KYC

[15] Reserve Bank of India, 'Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps'(November 2021) https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DIGITALLENDINGF6A90CA76A9B4B3E84AA0EBD24B307F1.PDF accessed 09th August 2023.

compliance for PPI accounts prior to loan disbursement, as well as the introduction of fundamental technological criteria for digital lending applications.

The RBI's directive has spurred discussions concerning the issues of financial inclusivity and credit accessibility. It is evident that the directive enhances transparency and responsible lending practices by mandating transparent information disclosure and robust credit evaluation procedures. Nevertheless, the prohibition of the PPI-linked channel for BNPL products has generated concerns about restricting the availability of convenient credit for a significant portion of the population lacking access to traditional credit sources. This emphasises the necessity of finding a delicate balance between protecting consumers and advancing financial inclusion.[16]

IV. Regulation in other jurisdictions

1. Australia

The Federal Government of Australia, on 21 November 2022, proclaimed its intention to regulate the BNPL products as credit products. In furtherance of this, the Treasury released a consulting paper with the proposed regulatory framework. The proposed framework envisages three models with varying degrees of intervention for regulating the BNPL products. *Option 1* provides for strengthening the BNPL Industry Code in addition to the affordability test. *Option 2* proposes the model for tailored limited regulations under the National Consumer Credit Protection Act 2009 (NCCPA). *Option 3* presents a stricter model for regulation under the NCCPA, which would require the BNPL service providers to hold an Australian credit license and would be subject to the same compliances as the ordinary licensed credit providers.[17]

After consultation, the Australian Government announced its intention to enforce *Option 2* under the BNPL Consultation Paper floated earlier, which will mandate the BNPL providers to hold an

[16] Meha Agarwal, 'How One RBI Notification Broke India's Fintech Dream' *Inc 42* <https://inc42.com/features/how-one-rbi-notification-shattered-hopes-of-indias-fintech-ecosystem/#:~:text=On%20June%2020%2C%202022%2C%20the,issuers%20and%20was%20effective%20immediately > accessed 09th August 2023

[17] Silvana Wood and Robert O'Grady, 'Buy Now Pay Later – Preparing for tougher regulation' (*Gilbert+Tobin*, 26th May 2023) <https://www.gtlaw.com.au/knowledge/buy-now-pay-later-preparing-tougher-regulation> accessed 21st August 2023.

Australian credit license. This move aims to include the BNPL services under the ambit of 'credit activity' defined under the NCCPA.[18] However, the BNPL providers will only be required to comply with the essential licensee obligations and have a more relaxed set of responsible lending obligations than what other credit licensees must abide by. Out of all the three options proposed in the BNPL consultation paper, this is the most balanced approach, which will moderately regulate the BNPL providers while fostering responsible lending practices.

Since 2021, BNPL providers in Australia have undergone regulatory changes under the Design and Distribution Obligations (DDO) framework outlined in the Corporations Act, 2001. These changes were introduced in response to the country's growing popularity and widespread usage of BNPL services. The DDO framework was extended to BNPL providers by broadening the definition of credit activities under the Australian Securities and Investments Commission Act, 2001 (ASIC Act). This extension means that BNPL providers are now considered as offering credit, which has important implications for their operations and obligations. One of the critical obligations is ensuring that their BNPL products are distributed to an appropriately identified target audience.[19] This is a significant departure from the previous approach, where BNPL providers primarily operated as payment facilitators rather than credit providers.

According to the law, companies are required to adopt a consumer-centric approach. They must create financial products that cater to the requirements of consumers in their designated target audience and deliver these products with precision. In cases where companies are not adhering to ethical practices, and there is a possibility of harm to consumers, ASIC now possesses the authority to intervene to stop improper behaviour and mitigate potential harm.[20] These regulatory changes represent a significant step towards ensuring responsible lending practices and consumer protection in the ever-changing financial industry.

2. Denmark

[18] ASIC, 'Credit' (*asic.gov.au)*<https://asic.gov.au/regulatory-resources/credit/> accessed 24th August 2023.

[19] Jim Boynton and Amanda Engles, 'ASIC FLEXING ITS DDO POWERS AND CRACKING DOWN ON TARGET MARKET DETERMINATIONS' (*King & Wood Mallesons*, 07th November 2022) <https://www.kwm.com/au/en/insights/latest-thinking/asic-flexing-its-ddo-powers-and-cracking-down-on-target-market-determinations.html> accessed 04th September 2023

[20] Rosalyn Teskey, 'Design and Distribution Obligations (DDO) and Product Intervention Powers (PIP)' (*deloitte.com*, 09 January 2019) <https://www.deloitte.com/au/en/services/audit-assurance/analysis/design-distribution-obligations-product-intervention-powers.html> accessed 26th September 2023

In May 2023, the Danish Government amended the Danish Consumer Credit Companies Act, (DCCCA) and the Danish Credit Agreement Act (DCAA) to include the credit provided by BNPL companies and regulate such products within its existing legal framework with the intention to provide increased consumer protection and tackle the problem of debt-traps. These amendments primarily involve an expansion of the types of credit agreements that fall under the purview of the laws. This aligns the regulation of companies offering BNPL services with that of banks and other lending institutions in Denmark.[21]

To begin with, the companies offering BNPL products and services will be required to obtain a consumer lending license from the Danish Financial Supervisory Authority (FSA), do regular creditworthiness assessments, and establish regulatory procedures to comply with the local consumer protection rules such as identifying the target group for each product. This implies that a consumer lending company can only create and provide products that align with the interests and goals of the identified target audience, by undertaking cost analysis and risk assessments.[22]

Previously, the DCAA and the DCCC excluded BNPL products that were interest-free and free of additional charges. However, with the legislative modification, the exemption for such BNPL products will be significantly narrowed, encompassing only credit agreements that meet all of the following criteria:

i. The agreement constitutes a contract for the purchase of goods or services.

ii. The deferred payment of the purchase price is devoid of any interest or charges.

iii. The deferred payment is directly provided by the seller of the goods or services, without involving any third-party credit provider.

iv. The deferment period extends no further than 90 days from the time of delivery.

While these amendments bring merchants and third-parties actively providing credit within its scope, the third-parties who function solely as intermediaries connecting consumers with credit

[21] Stefan Agergaard Hansen , 'Danish Government looks at stricter regulation of Buy-Now-Pay-Later products' (*monthio.com*, 26 June 2023) <https://www.monthio.com/post/danish-government-looks-at-stricter-regulation-of-buy-now-pay-later-products> accessed 23rd September 2023

[22] Rasmus Mandoe Jensen, 'New bill to regulate "buy now pay later" credits' (*plesner.com*, 04 July 2022) <https://www.plesner.com/insights/articles/2022/07/new-bill-to-regulate-buy-now-pay-later-credits?sc_lang=en> accessed 23rd September 2023

providers, without actually extending credit themselves, do not fall under the purview of the DCCA and DCCCA.[23]

3. Hong Kong

While there is no separate legislation to regulate the BNPL products in Hong Kong, these are regulated within the existing legislations. In September 2022, the Hong Kong Monetary Authority (HKMA) issued a circular titled ”Enhancing Consumer Protection in Respect of ‘BNPL’ Products”.[24] The circular provides for mechanisms to increase consumer protection for such type of credit lines which includes mandating banks to incorporate a message to consumers in the promotional content, requesting them to borrow responsibly.

In addition, the promotion must disclose that the products offered are credit products, to avoid the misrepresentation that buying these would not involve borrowing. Another disclosure requirement is to clearly mention the interest charges and reflect them in the annual percentage rate for the reference of the consumer. Further banks would be held accountable under the local consumer protection laws for the acts of third-party collaborators.

Banks also need to include in the Key Facts Statement of a BNPL product that any delay in repayment could have a negative impact on the credit score of the consumer. Moreover, banks must ensure that customers are adequately informed about the applicability and process of chargebacks for BNPL products and if the BNPL option is available via a bank’s credit card product, consumers ought to receive identical chargeback safeguards. While reviewing the applications for BNPL products, banks are required to evaluate the creditworthiness.

The non-banking institutions and other such institutions which do not hold a banking licence, but seek to provide BNPL services, fall within the scope of Money Lenders Ordinance, 1911 (Cap. 163). Subject to which such institutions are required to obtain a money lenders licence. Part IV of this ordinance prohibits and penalises lending at any effective rate of interest exceeding 48%

[23] Claudia Mortensen and Annette Printz Nielsen, ‘Buy Now Pay Later Regulatory Tracker’ (*twobirds.com*) <https://www.twobirds.com/en/trending-topics/buy-now-pay-later-regulatory-tracker/denmark> accessed 24th September 2023

[24] Hong Kong Monetary Authority, ‘Enhancing Consumer Protection in Respect of “Buy Now, Pay Later” Products’ (September 2022) <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220902e1.pdf> accessed 24th September 2023.

per annum[25] and considers any payment of interest on loan exceeding 36% to be exorbitant (unless found reasonable by the court)[26]. Further, similar disclosure requirements for advertisements as mentioned in the circular are applicable.

V. Comparative analysis

1. Australia

India's regulatory directive, while enhancing transparency and responsible lending, has raised concerns about limiting the availability of convenient credit, particularly for those who lack access to traditional credit sources. This highlights the challenge of balancing consumer protection with advancing financial inclusion. Australia's approach aims to strike a balance between regulation and responsible lending practices. While it requires BNPL providers to hold a credit license, it does not impose the same level of obligations as traditional credit providers. This approach aims to regulate BNPL while still allowing the industry to thrive and provide accessible credit to consumers.

India's regulatory response focused on discontinuing the practice of loading PPIs from credit lines. The directive by the RBI prohibited this practice, which was prevalent among PPI operators. The emphasis here is on ensuring that PPI operators do not provide credit via this method. While Australia's approach involves requiring BNPL providers to hold an Australian credit license. This means that BNPL operators are treated as credit providers, and they need to comply with essential licensee obligations. While this regulatory approach is more interventionist, it still allows for a degree of flexibility compared to traditional credit providers, acknowledging the unique nature of BNPL services.

In contrast to India, Australia has taken a more flexible regulatory approach. The proposed regulatory framework includes three distinct models with varying degrees of intervention. The choice of Option 2 means that BNPL providers will need to hold an Australian credit license, but with a more relaxed set of responsible lending obligations compared to traditional credit providers. Australia's regulatory framework emphasizes a consumer-centric approach. BNPL providers are required to create financial products that meet the needs of their designated target

[25]Money Lenders Ordinance 1980, s 24(1).
[26]Money Lenders Ordinance 1980, s 25(3).

audience. This approach underscores the importance of aligning financial products with consumer requirements to prevent harm and promote responsible lending.

Thus, India and Australia have taken different regulatory approaches to address the challenges associated with BNPL services. India's approach is characterized by centralized regulation through a directive issued by the RBI, with an emphasis on KYC and underwriting procedures. Australia, on the other hand, has opted for a more flexible and tiered regulatory approach that requires BNPL providers to hold a credit license, but with less stringent obligations compared to traditional credit providers. Both approaches aim to enhance transparency and responsible lending, but they reflect the unique regulatory landscapes and priorities of each country.

2. Denmark

Denmark's regulatory framework places a strong emphasis on consumer protection. The amendments narrow exemptions for BNPL products, ensuring that consumer interests are well-preserved. Companies offering BNPL products in Denmark are mandated to identify specific target groups for each product and align their offerings with the interests and financial capacities of these identified audiences. This targeted approach underscores tailoring products to meet consumers' needs and affordability.

The regulatory changes in Denmark bring greater clarity to the BNPL sector. Companies must acquire a consumer lending license, conduct regular creditworthiness assessments, and adhere to local consumer protection rules. This robust framework is designed to reduce the risk of consumers falling into debt traps. Denmark's approach meticulously defines the criteria for exemption of certain BNPL products. These criteria, such as the 90-day deferment period and direct seller-provided financing, ensure that only products meeting specific conditions remain exempt from regulation. This prevents potentially exploitative products from evading oversight.

While India's regulatory approach is characterized by its comprehensiveness and its focus on creating a comprehensive framework for the PPI sector. It addresses issues related to credit lines, encourages innovation, and emphasizes the need for transparency. Denmark's regulatory approach is more targeted and prescriptive. It prioritizes consumer protection, responsible lending, and risk assessment within the BNPL sector. The emphasis is on preventing debt traps and ensuring that BNPL products are aligned with consumers' financial capacities.

Both countries acknowledge the importance of safeguarding consumer interests. However, India's approach is broader in scope, while Denmark's approach is more specific and detailed. India's regulatory approach highlights the challenge of balancing consumer protection with the goal of extending financial inclusion, especially for individuals without access to traditional credit sources.

Denmark's approach is designed to mitigate risks associated with BNPL products by limiting exemptions and ensuring that these products are tailored to meet consumers' needs.

3. Hong Kong

First, India has taken a more cautious approach, with the RBI prohibiting the loading of PPIs from credit lines. This effectively means that BNPL providers can no longer offer BNPL products through PPIs. In contrast, Hong Kong has taken a more moderate approach, with the HKMA issuing a circular to banks and non-banking institutions on how to enhance consumer protection for BNPL products. This circular provides for a number of measures, such as mandating disclosure of key information and requiring banks to assess the creditworthiness of customers before granting them BNPL loans.

Second, India's regulations are more comprehensive in terms of the scope of BNPL products that they cover. The RBI's directive applies to all PPI operators, whereas the HKMA's circular is only applicable to banks and non-banking institutions that hold a money lenders licence. This means that there is a regulatory gap for BNPL products offered by other types of institutions in Hong Kong.

Third, India's regulations are more prescriptive in terms of the specific requirements that BNPL providers must comply with. For example, the RBI's directive prohibits BNPL providers from charging late fees, while the HKMA's circular does not include such a prohibition. Overall, India's BNPL regulations are more cautious and comprehensive than Hong Kong's. However, Hong Kong's Regulations are still evolving, and it is possible that the HKMA will introduce stricter regulations in the future.

VI. Way Forward

India's BNPL sector is at a crossroads, facing the need for regulatory balance that ensures consumer protection, financial inclusion, and responsible lending practices. To move forward, several innovative recommendations can be considered, By implementing these recommendations, India can strike a balance between promoting financial inclusion, protecting consumers, and fostering innovation in the BNPL sector. This will help ensure that BNPL services continue to play a positive role in India's evolving financial ecosystem.

1. Collaborative Industry Standards:

Industry-wide standards for BNPL providers can help to ensure responsible lending, transparent pricing, and consumer education. The standards could include mandatory affordability checks[27] before extending credit to a customer or mandating BNPL providers to limit the amount of credit they extend to a customer based on their debt-to-income ratio limits, which could be determined basis ratio of customer's monthly debt payments to their monthly income.[28] These standards can be developed through collaborative efforts between regulators, fintech firms, and consumer advocacy groups.

2. Alternative Data Usage and Credit Scoring Innovation:

Use of Alternative Data helps in wider coverage of data, such as utility bill payments, rental history, and social media activity, to assess creditworthiness. This can be used to assess creditworthiness and expand access to credit for underbanked populations. However, it is important to use alternative data responsibly and ethically[29]. While Traditional Credit Scoring relies on factors such as credit history, employment history, and income to assess a person's creditworthiness. This can make it difficult for people with little or no credit history to obtain loans. Alternative credit scoring models can help individuals to establish a credit history and

[27] Ellie Lugt and Dr. Bobby Stuijfzand, 'Buy Now Pay Later: What are the risks and benefits to consumers?' (*Behavioural Insights Team*, 29th June 2023) <https://www.bi.team/blogs/buy-now-pay-later-what-are-the-risks-and-benefits-to-consumers/> accessed 06th October 2023.

[28] 'What is a debt-to-income ratio?' (*consumerfinance.gov*, 28th August 2023) <https://www.consumerfinance.gov/ask-cfpb/what-is-a-debt-to-income-ratio-en-1791/#:~:text=Your%20debt%2Dto%2Dincome%20ratio,will%20have%20different%20DTI%20limits? accessed 06th October 2023

[29]International Committee On Credit Reporting, 'Use of Alternative Data to Enhance Credit Reporting to Enable Access to Digital Financial Services by Individuals and SMEs operating in the Informal Economy' (June 2018) <https://www.gpfi.org/sites/gpfi/files/documents/Use_of_Alternative_Data_to_Enhance_Credit_Reporting_to_Enable_Access_to_Digital_Financial_Services_ICCR.pdf> accessed 06th October 2023.

access more traditional financial services[30]. These models can consider a wider range of factors, such as payment behaviour on BNPL platforms. For example, some fintech firms are developing alternative credit scoring models that consider factors such as social media activity and purchase history.

3. Digital Financial Literacy Programs:

Digital financial literacy campaigns can help consumers to understand BNPL products, their terms, and potential risks. These campaigns can be delivered through a variety of channels, such as online courses, social media, and community outreach programs. For example, RBI has launched a digital financial literacy program called "Sachet".[31] This program provides educational resources on a variety of topics, including BNPL, credit cards, and digital payments.

Research and Data Analysis:

Research and data analysis can help to assess the impact of BNPL services on financial inclusion and consumer protection. Data collection and analysis is strength of any FinTech company, every single data point – alternative data, direct consumer (device) data, research bureau, account aggregator or public entities – is important in the lending business. Credit model is always evolving and having more variables can help in decision making process as they assist in predicting probability of default on payments. This information can be used to refine regulations and policies as needed. For example, the RBI established a working group to review the regulatory framework for fintech which came out with recommendations in its report for digital banking.[32]

4. Consumer-Focused Regulatory Sandbox:

[30]Lendfoundary, 'What is Alternative Credit Scoring & Why is it So Popular?' (*lendfoundary*, 09th July 2020) <https://lendfoundry.com/blog/what-is-alternative-credit-scoring-why-is-it-so-popular/#:~:text=Alternative%20credit%20scoring%20helps%20people,start%20establishing%20their%20credit%20scores> accessed 07th October 2023.

[31] Reserve Bank of India, 'FAQs-Integrated Ombudsman Scheme, 2021' (*rbi.org.in*, 01st January 2023) <https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=3407> accessed 07th October

[32] ibid 6.

A regulatory sandbox can allow innovative fintech firms to test new products and services in a controlled environment.[33] This can help to accelerate innovation and promote financial inclusion. For example, the RBI has established a regulatory sandbox for fintech firms to test new products and services related to digital payments, blockchain, and artificial intelligence.[34]

5. Sustainable Global Practices:

BNPL providers should adopt sustainable lending practices, such as promoting responsible lending, offering debt counselling services, and implementing measures to prevent over-indebtedness. This is important to protect consumers from financial harm. For example, some fintech firms are offering debt counselling services to help consumers manage their finances and avoid over-indebtedness. India can learn from regulatory approaches in other countries to develop a balanced and effective regulatory framework for the BNPL sector. For example, Australia has a significant departure from the previous approach, where BNPL providers primarily operated as payment facilitators rather than credit providers, Hong Kong has penalised lending at exorbitant interest rates, and Denmark has narrowed licensing criteria, which excludes those involving any third-party credit provider.

[33]Giulio Cornelli, Sebastian Doerr, Leonardo Gambacorta and Ouarda Merrouche 'Regulatory sandboxes and fintech funding: evidence from the UK' (2020) BIS Working Papers No 901 https://www.bis.org/publ/work901.pdf accessed 05th October 2023

[34] Shashidhar K.J., 'Regulatory Sandboxes: Decoding India's Attempt to Regulate Fintech Disruption' (2020) ORF Issue Brief No. 361 https://www.orfonline.org/wp-content/uploads/2020/05/ORF_Issue_Brief_361_Fintech.pdf accessed 05th October 2023

UNDER THE FINFLUENCE: STRATEGIES FOR A BALANCED REGULATORY APPROACH- REGULATORY FRAMEWORK FOR FINTECH IN INDIA

- *Gayatri Barua Nambyar& Maanya Sharma*[1]

Abstract

With the rise of social media and online platforms, individuals with financial expertise have emerged as influential voices, capable of shaping investor sentiment and behaviour. This article takes a look into the dynamic world of financial influencers and their growing impact on investment decisions in the digital age. While many are genuinely qualified and educated, others work as unregistered Investment Advisers (IAs) or Research Analysts (RAs). There is an apprehension that these finfluencers receive consideration in an undisclosed manner in exchange for advertising specialised financial products, services, or securities. As a result, there may be potential conflicts of interest and biased financial advice.

However, this may deter them from delivering meaningful information, potentially prioritizing personal gains over followers' benefits. The delicate balance required to encourage financial innovation while safeguarding investor interests is discussed along with policy changes that are required to ensure investor protection and maintain market integrity. SEBI's efforts to regulate financial influencers signify a crucial step toward enhancing transparency and accountability in the fintech-driven landscape. The proposed regulatory framework, if implemented thoughtfully, can nurture a conducive environment for financial influencers while mitigating risks and protecting the financial well-being of investors.

Keywords: *Financial Influencers, SEBI, Investment Advisors, Regulatory framework, Informed decisions.*

[1] 4th Year, BBA.LLB., St. Joseph's College of Law. Gmail: gayatri.nambyar@gmail.com&maanyash280@gmail.com

I. Introduction

The advent of "*fourth screen technology*", which includes smartphones and tablets, revolutionised both, how mobile platforms approach the world of social networking as well as how we, as a society, communicate widely[2]. Many of these websites started out as a way to connect with old acquaintances or classmates through social networking. The main social media sites, however, have recently developed into "*home to a variety of subcultures and microgenres—including financial advice*"[3].

The frequency with which particular hashtags are viewed or searched by users on social media sites can be used to monitor how people really "*use*" those platforms. For instance, hashtags play a useful role on TikTok, a social media platform where users create and share short videos, as they serve as a genuine, practical organising concept for monitoring distinct blobs of activity[4]. Although, Tik-Tok is well known for having a significant following among young adults, financial information, notably investing advice, has recently become one of the most well-liked "*blobs of activity*" to appear on the platform[5]. In addition, to the emergence of cryptocurrencies, blockchain, non-fungible tokens (NFTs), and other Web3 financial supplements, the development of novel financial technology (fintech) has also led to the rise of "*finfluencers*".

According to a study by the National Centre for Financial Education[6], only 27% of the population is financially literate, indicating a shockingly low level of financial literacy. Financial influencers have recently played a significant role in bridging this gap. Finfluencer's use of clear, laymen-friendly language has been of great help in the fight against financial illiteracy. Having stated that, the heavy dependence and unwavering confidence placed in Finfluencers, along with

[2] Saqib Shah, The History of Social Networking, Digital trends (May 14, 2016), https://www.digitaltrends.com/computing/the-history-of-social-networking/ last visited on August 02, 2023.
[3] The Finfluencer Boom, Agency P'ship (March 21, 2021), https://perma.cc/KKN2-VHQR last visited August 04, 2023.
[4] John Herrman, How tiktok is rewriting the world, NY Times, (March 10, 2019) https://www.nytimes.com/2019/03/10/style/what-is-tik-tok.html
[5] Sophie Kiderlin, Social media has hooked young investors on finance, but a growing number are taking more and more risks. 'Finfluencers' and money experts say it's time for some caution, INSIDER (July 18, 2021), https://markets.businessinsider.com/news/stocks/gen-z-investing-social-media-finance-fintok-millennial-investors-2021-7 last visited on August 05, 2023.
[6]National Strategy for Financial Education 2020-25, Cl.10

the unrestricted, unhindered freedom given to such content providers, create a remedy for sceptics to deceive innocent, gullible individuals. The financial information that many freelancers and influencers in the digital age provide is appealing to the new generation of retail investors because it is simplified and easy to understand. This category of investors intends to make quick money without dedicating lengthy hours in market research. However, certain YouTube influencers have occasionally been exposed for stock price manipulation. The Securities and Exchange Board of India (SEBI) issued stringent instructions to discontinue their participation in the Indian securities market.

Additionally, the influencer-follower relationship's inherent power dynamic may make customers more vulnerable, especially in the case of one-sided para social relationships. In these one-sided, para social relationships, the financial influencer, who may not even be aware of the follower's existence, provides emotional support and interest to the follower. Even if they are unqualified or unlicensed to offer financial advice, these connections can increase the follower's degree of trust, credibility, and reliance on the suggestions and advice of financial influencers. Retail investors who lack financial knowledge may be more susceptible to the hazards offered by finfluencers, making this potentially risky for them.

It may not necessarily pose a problem for young people to learn how to handle their finances through social media. Recent occurrences and deliberation, however, have brought attention to the idea that social media and trade apps combined may "*be doing more harm than good*," considering that they may not be the most inclusive environments and may not give young users sufficient instructional content. These potentially harmful factors are made worse by the overall absence of oversight over individuals that provide online financial advice to potentially thousands, if not millions, of investors and are known as "*finfluencers*." Financial services professionals are not surprised by this group's increasing popularity because, as one finance analyst puts it, "*if you're using social media and you have a choice between simple 30-second tips from a finfluencer who makes it sound foolproof, or sensible advice from a regulated firm,*

complete with reams of risk warnings that make it all sound terrifying, the temptation is to opt for the former."[7]

However, as their power increases, so do the risks associated with their unregulated financial advice. Financial malpractice cases involving influencers have been on the rise in India as well as around the world. Recent cases have highlighted the urgent need to regulate these financial influencers in order to protect investor interests and uphold the integrity of financial markets[8].

One of the major issues with these unregulated advisors is that many finfluencers lack necessary financial qualifications and expertise, which leads to the spread of inaccurate and misleading information. Secondly, the potential for conflicts of interest is very high, since influencers often promote certain financial products or services in exchange for compensation without disclosing these affiliations to their audiences. This compromises the impartiality of their advice. Thirdly, the rapid and viral nature of social media amplifies the spread of speculative and high-risk investment strategies, giving rise to a culture of short-term gains over long-term financial stability.

With the development of Finfluencers, proposals for regulation have been made in India as well as other nations due to concerns raised by the absence of monitoring by finfluencers, such as the increased possibility of market volatility and exploitative practices. New Zealand is one of the nations that is leading the charge in tackling this problem. It recently implemented new financial advisory rules that could serve as a model for other nations as they start to address problems with their own governance structures[9].

In India, however, the regulations are still new and in the making. The Securities Exchange Board of India has recently introduced various regulations to govern these financial influencers. The crackdown on these finfluencers comes as a response to the rise in the number of cases of financial misconduct by these self-proclaimed experts. Regulation is essential in order to ensure transparency and protect consumers from fraudulent or manipulative practices.

---

[7] Shane Hickey, *As Finfluencers' Spread Through Social Media, Beware the pitfalls,* GUARDIAN (Aug 2021),https://www.theguardian.com/money/2021/aug/22/as-finfluencers-spread-through-social-[https://perma.cc/DC4F-4AZE]

[8]*Navigating the Realm of Financial Influencers: A Quest for Regulation*, Tax Guru, (October 21, 2023) https://taxguru.in/sebi/navigating-realm-financial-influencers-quest-regulation.html

[9]Gabriel Olano, *FMA releases guide for 'finfluencers'*, Financial Markets Authority (June 28, 2021)

II. The Current Regulatory Framework

Influencers work in legal grey areas where it's not always explicit what counts as advertising and what needs to be disclosed. Financial influencers need to be subjected to regulation, because they offer regulated financial products and services to their audience, such as investment funds or general financial advice, which has an enormous impact on people's financial decisions. According to the Consultation paper released by SEBI, influencers are typically unregistered entities that engage their numerous followers with engaging material, information, and guidance on a range of financial concerns. While some finfluencers may act as registered Investment Advisors (IA) or Research Analysts (RA), the majority are unregistered entities and are frequently connected to an intermediary or SEBI-registered entity.

The '*Guidelines for Influencer Advertising in Digital Media*' issued by Advertising Standards Council of India (ASCI) describes 'influencers' as "*someone who has access to an audience and the power to affect their audiences' purchasing decisions or opinions about a product, service, brand or experience, because of the influencer's authority, knowledge, position, or relationship with their audience*".

Finfluencers currently fall into a regulatory "*grey area*." According to Regulation 3 of the SEBI (Investment Advisors) Regulations, 2013[10], it is unlawful for anybody to represent themselves as an IA or RA without first obtaining a certificate of registration from SEBI.

Further, Regulation 2(1)(m), "*investment adviser*" refers to any individual who, for a consideration, engages in the business of offering investment advice to clients or other individuals or groups of individuals. This definition also includes any individual who presents himself as an investment adviser, regardless of the name used. It may be argued that since a Finfluencer's advice is typically without any consideration, open to all and accessible to the general public, they do not meet the criteria of "*investment adviser*."

In accordance with Regulation 2(1)(l) of the IA Regulations, "*investment advice*" refers to guidance or advice for buying, selling, investing in, or otherwise transacting in securities or investment products, as well as recommendations for investment portfolios that contain securities

[10] Securities and Exchange Board of India (Investment Advisers) Regulations, 2013 [Last amended on August 18, 2023], No. LAD-NRO/GN/2012-13/31/1778 last visited on Aug 30, 2023.

or investment products. These tips may be made orally, in writing, or through any other means of communication for the client's benefit, and they must also include financial planning. It is made clear in the caveat to this definition that "*Provided that investment advice given through newspaper, magazines, any electronic or broadcasting or telecommunications medium, which is widely available to the public, shall not be considered as investment advice for the purpose of these Regulations.*" In certain aspects, the rule itself, namely the proviso to Regulation 2(1)(l), precludes the Finfluencer from the meaning of "*investment advice*."

It is stated in Regulation 4 that the IA Regulations do not apply to "*Any person who gives general comments in good faith regarding trends in the financial or securities market or the economic situation where such comments do not specify any particular securities or investment product*."

For IA certification, Regulation 7 of the IA Regulations specifies particular educational qualifications as well as a minimum of five years of experience in activities connected to advice on financial products or securities, fund, asset, or portfolio management. Similar educational and professional requirements are listed in the RA Regulations[11] as prerequisites for registration as a research analyst.

Additionally, on January 25, 2022, Regulation 4 of the PFUTP (Prohibition of Fraudulent and Unfair Trade Practices Relating to Securities Market) Regulations, 2003[12] was changed to accommodate "*disseminating information or advice through any media, whether physical or digital, which the disseminator knows to be false or misleading in a reckless or careless manner and which is designed to, or likely to, influence the decision of investors dealing in securities*" within fraudulent or unfair trade practices. Through the Interim Order in the matter of *Svarnim Trade Udyog Limited* in January 2022, SEBI identified that stock suggestions made on the social media platform Telegram had resulted in market manipulation[13]. It ought to be recognised that the aforementioned directives do not outline SEBI's regulatory intentions with regard to finfluencers.

[11] Securities and Exchange Board of India (Research Analysts) Regulations, 2014 [Last amended on August 03, 2021], No. LAD-NRO/GN/2014-15/07/1414.
[12] Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices Relating to Securities Market) Regulations, 2003
[13] Interim Order in the matter of Svarnim Trade Udyog Limited (Jan 31, 2023), WTM/SM/ISD/ISD-SEC-4/23412/2022-23

Finfluencers can be categorised as falling under the definition of 'Research Analyst,' as per Regulation 2(u) of the "*SEBI (Research Analysts) Regulation, 2014*." They are therefore responsible for its content in compliance with the applicable laws. The definition specifies that an individual qualifies as a 'Research Analyst' if they prepare or release research reports, furnish research reports, express opinions on public offerings, or provide price projections. These regulations also stipulate the necessity of possessing technical qualifications and successfully completing the National Institute of Securities Market (NISM) examinations. These Regulations help in establishing a protective measure for investors and fulfil the core objectives of SEBI.

III. The Crackdown on Finfluencers

In a recent case, Ms Gunjan Verma, a financial influencer was penalised by the SEBI for providing unregistered investment advice online. This action comes as a part of SEBI's crackdown on unregistered finfluencers on social media. A complaint was filed by one Megha Jain who claimed that Verma had taken a sum of Rs. 2.5 Lakhs from her to invest on her behalf. Verma promised to invest this money in the stock market and guaranteed profits on the same. It was claimed that Verma mentally harassed the complainant when she asked for a refund of the money.[14] Following the receipt of the complaint, SEBI advised Verma to provide information regarding the fees she has collected from all her other clients. After examination, it was observed that Verma was not registered with SEBI as an intermediary. Furthermore, there was ample evidence to prove that Verma collected money from the complainant as well as other clients. Therefore, it was clear that she had received consideration from the clients for the service provided by her.

An order was issued by the Securities and Exchange Board of India imposing a fine of Rs 1 Lakh on Gunjan Verma for providing unregistered investment advice. According to the regulations, only advisors who get themselves registered and verified with SEBI are to be called Registered Investment Advisors (RIA) and are permitted to offer investment advice to investors. It was found that Verma had been providing unregistered investment advice online since 2018. She has

[14] *Who is Gunjan Verma, and Why Was She Penalised by SEBI?*, Indiacsr, (May 27, 2023),https://indiacsr.in/unraveling-the-identity-of-gunjan-verma/.

been penalised for the same and has been instructed to refund the fees which she has charged her clients so far.[15]

In another case, SEBI imposed a ban on influencer and self-proclaimed stock market expert, Mohammad Nasiruddin Ansari, popularly known as "*Baap of Chart*", prohibiting him from buying, selling or dealing in the securities market until further notice. SEBI's order states that Ansari sold his stock suggestions while passing them off as educational training. His company offered over 19 courses including some that claimed to offer guaranteed returns. The influencer is also ordered to refund a sum of Rs.17.2 crore which he allegedly made by misleading investors and influencing them to deal in securities.[16]

In May 2023, SEBI fined P R Sundar and his company more than INR 6 crore and forbade them from carrying on his business for a year. P R Sundar provided a variety of tailored packages for their investment advisory services through a blog. He has over a million followers on YouTube and hundreds of thousands on Twitter. Without being registered with SEBI as an investment advisor, P R Sundar was advising various individuals to buy, sell, and deal in securities through his firm, i.e., giving investment advice in accordance with IA Regulations.[17]

IV. An Analysis of Sebi's Consultation Paper on Finfluencers

After witnessing a rise in the number of unregistered advisors on various social media platforms such as Facebook, Telegram, YouTube, Instagram and X (formerly Twitter), the market regulator is now working on framing guidelines to govern these unregulated influencers. There is a lot of ambiguity regarding the qualifications, expertise and credibility of these unregistered advisors. They foster highly unrealistic expectations about earning profits in the market. Furthermore, they often provide biased advice which benefits them through advertisements, profit sharing, equity, referral fees, etc. On 25th August, 2023, a consultation paper on "*Association of SEBI Registered Intermediaries/Regulated Entities with Unregistered Entities*

[15] Securities and Exchange Board of India, Order in the matter of unregistered investment advisory by Gunjan Verma, (Issued on May 26, 2023).
[16] *Explained: Here's Why SEBI Banned 'Baap Of Chart' Owner From Trading*, NDTV NewsDesk, (October 27, 2023), Explained: Here's Why SEBI Banned 'Baap Of Chart' Ownernasiruddin Ansari From Trading (ndtv.com)
[17] Smita Jha, Nikita Nagori and Anushri Uttarwar, *FINFLUENCERS, BEWARE!*, Khaitan and Co. (August 9, 2023) https://www.khaitanco.com/sites/default/files/2023-08/Finfluencers%20beware!%2009082023.pdf

(including Finfluencers)" was published by SEBI. This paper defines what a finfluencer is and proposes guidelines to regulate them.

The following are the key proposals that were made in the consultation paper-

1. Regulated entities will not be connected to unregistered entities- SEBI highlighted the problems with unregistered finfluencers, who may persuade their followers to buy items, services, or stocks in exchange for income from platforms or producers that is not disclosed to the followers. As a result, it realised the need to limit the flow of such payments between registered intermediaries and unregistered entities. SEBI believes that if an entity is regulated under it, then all its associated entities must be regulated as well. It was also noticed that many registered entities make use of unregistered individuals to promote their products and services. This paper proposes that entities regulated by SEBI such as exchanges, brokers, mutual funds etc, will not be allowed to be associated with any unregistered entity through any medium including advertisements, profit sharing, equity or referral fees.

2.Confidential information- SEBI has identified data protection as one of the key areas in which reform is necessary. Confidential information of clients is of utmost importance and therefore must not be accessible to or shared with any unregistered entities. In the paper, it has proposed that sharing of Confidential information of clients of registered entities with any unregistered entity must be prohibited.

3. Inducements will be considered as fraudulent practices- Finfluencers often use creative and catchy content to entice people to invest in certain stocks. The paper proposes that such an inducement by making promises of guaranteed high profits will be considered as fraudulent. However, investor education is an important objective of SEBI and therefore it is important to note that individuals providing genuine education and financial literacy about the markets are permitted to continue to do so and this will not be considered as fraud.

4. Advisors must be registered with SEBI- The market regulator has highlighted the importance of creating a regulated and controlled community of financial advisors online. All unregistered entities will be prohibited from giving any sort of financial investment advice to clients. As per

SEBI (Investment Advisers) Regulations, 2013, any person who gives advice, stock recommendations, portfolio recommendations, etc; must be registered with SEBI.

5. Transparency ("material disclosures")-Registered entities must disclose their registration details such as their registration number, contact details, and an investor grievance redressal helpline as well as other appropriate and relevant information. It is important for registered entities to disclose such information as it prevents unlawful activities such as fraud and misconduct as well as the spread of misinformation. They must also make appropriate disclaimers regarding their vested interests such as disclosure of any consideration that they may receive in exchange for advertising the products or services of a company.[18]

The main objective of this consultation paper is to regulate the connection between unregistered entities and the regulated entities in order to promote their products and services. It was found that a lot of these so-called finfluencers were inducing their followers to purchase products without disclosing whether or not they would receive any compensation for such a promotion.

Furthermore, SEBI has also directed the registered entities to actively dissociate themselves from these unregistered finfluencers and also encouraged them to file criminal charges under Section 420 of the Indian Penal Code, 1860 against any finfluencer who associates themselves with a registered entity. The consultation paper proposes to curb fraudulent practices adopted by finfluencers by disrupting their revenue model. It aims to ensure that online advisors are trustworthy, transparent and unbiased in terms of the information they give to their followers and subscribers. The protection of the interests of investors remains to be a priority.[19]

Even though the consultation paper on regulating finfluencers represents a landmark development in the Indian financial market, implementing it effectively presents certain challenges. Defining "*material disclosures*" and effectively managing a vast number of finfluencers will require careful consideration. Furthermore, collaboration with technology platforms will be crucial to streamline disclosure processes and conflict-of-interest checks.

[18] Securities and Exchange Board of India, Consultation Paper on Association of SEBI Registered Intermediaries/Regulated Entities with Unregistered Entities (including Finfluencers), (Issued on August 25, 2023).
[19] Megha Mishra, *ETtech Explainer: Decoding the buzz around Sebi's finfluencer guidelines*, The Economic Times, (Sept. 07, 2023, 8:15 AM IST), https://economictimes.indiatimes.com/tech/technology/ettech-explainer-decoding-the-buzz-around-sebis-finfluencer-guidelines/articleshow/103435126.cms last visited on Sept 02, 2023.

It is important to note that SEBI's approach is not happening in isolation. Regulating finfluencers is a global concern, with many countries grappling with similar issues. SEBI's framework can serve as a valuable example, and its success will be watched closely by other financial regulators around the world.

V. Impact on Retail Investors and Financial Influencers

In order to understand the impact of these guidelines on influencers, we must first understand the revenue model that is adopted by them. A majority of these finfluencers earn their money through commissions, brokerage or advertisements. Companies offer commissions to such influencers in exchange for advertisements or promotions done by the individual. The companies often issue referral codes to the finfluencer which can be used by clients while purchasing the product that is promoted. Each time someone uses this referral code to purchase a product, the finfluencer earns a percentage of the revenue earned by the company on that sale. Therefore, these finfluencers usually have a personal interest in selling a product.

The rules issued by SEBI essentially destroy the revenue model adopted by many finfluencers. It bans the use of commissions, brokerage, referral code, affiliate links and any other ways through which regulated entities have associated themselves with unregistered entities (the finfluencers). This ensures that the financial advice given to investors is free from any biases or personal agendas.

In an interview with CNBC TV, a popular finfluencer Sharan Hegde stated that the finfluencer community views this initiative by SEBI as a welcome move as it will allow regulation of the fraudulent finfluencers who provide misinformation to induce people to invest in certain stocks. He further talked about how the majority of finfluencers do not actively promote products that are registered under SEBI, and therefore believes that the new regulations are unlikely to have a significant impact on a majority of the finfluencers.

However, this move by SEBI will greatly benefit retail investors. Investors will witness an enhanced level of transparency in the market, which will not only allow them to make more informed investment decisions, but also help them protect themselves from becoming victims of fraud or misinformation. The SEBI believes that it is the responsibility of the finfluencers to disclose their interests before making any kind of recommendations to their clients. This allows

the clients to be more aware of the interests of the advisor, which allows them to recognize and protect themselves from any kinds of bias that the finfluencer may have while giving advice. Furthermore, the paper aims to eliminate the problem of lack of accountability of finfluencers. Following the proposed rules, the finfluencers must now be mandatorily registered under SEBI and can therefore be easily held accountable for any misconduct or fraudulent practices. In the event of any violations, the guidelines also encourage filing of criminal charges under Section 420 of the Indian Penal Code. Such registration also implies that the market regulator can ensure that only those individuals who possess the necessary qualification and skills can be registered as financial advisors.[20]

VI. Recommendations For Sebi's Regulatory Framework

1. Content review and approval- It involves establishing a process through which regulators or designated agencies review and approve financial data generated and distributed by financial influencers before it becomes available to the public. This process serves several purposes:

a.Quality control: Content reviews and approvals ensure that financial advice and recommendations provided by finfluencers meet certain quality standards. This includes accurate reporting of financial information, compliance with legal guidelines, and responsible use of information.

b.Investment Protection: By reviewing and approving content, regulators can identify and prevent unfair, misleading, or potentially harmful financial advice that could adversely affect investors. This protects investors from making uninformed investment decisions based on unreliable information.

c.Compliance Verification: The audit process helps ensure that financial influencers are complying with regulatory requirements. Ensures that they do not make unauthorized disclosures, make unsubstantiated statements, or engage in practices that violate existing financial regulations.

Review and approval processes may vary in size and scope depending on the regulatory framework established and specific requirements set by the regulatory authority. Some

[20] Rajiv Rajan Singh, *SEBI paper hits at 'Finfluencer' menace*, Fortune India, (Sept. 04, 2023),https://www.fortuneindia.com/investing/sebi-paper-hits-at-finfluencer-menace/113969 last visited on Sept 10, 2023 .

jurisdictions focus on a holistic review with prior approval, while others may conduct randomised or targeted checking. Overall, internal review and approval is a proactive measure to protect the interests of retail investors, maintain the integrity of financial markets, and ensure that financial influencers will provide reliable and accountable financial information to the public.

2.Continuous education – It refers to an ongoing pursuit for knowledge and skill. Lawmakers should encourage financial influencers to maintain and upgrade their financial literacy. It involves an in-depth understanding of financial markets, investments, risk management, and other related financial topics. SEBI can provide the registered financial influencers with a continuous education in order to help them stay updated and informed about the new and ever-changing market trends. It will enable them to keep up with the changing market and thus allow them to provide more reliable and accurate financial advice to their clients. A continuous education also helps to ensure that their knowledge and skills are not outdated and inaccurate. This can be done by conducting periodic and recurring seminars, workshops or conferences organised by the SEBI or other related authorities.

Their education or certification should have an expiration period, after which finfluencers must renew their certification by completing updated training or passing recertification exams. This ensures that they are updated with the current economic trends and regulations. Certified peer influencers are more likely to be trusted by their audience, as certification acts as a marker of professionalism and competence.

3.Complaint mechanism- The market regulator can also set up a complaint mechanism through which investors may directly file complaints about fraudulent activities as well as other grievances. This can be done by creating an authority specifically for the purpose of hearing complaints, investigating such complaints and imposing penalties on the defaulters. Establishing a complaint mechanism will make grievance redressal much easier and faster. A speedy and just system is essential in order to safeguard the interests of the investors.

4.Enforcement mechanisms-They are those processes which ensure compliance with laws. These mechanisms are used in order to enforce rules and ensure that they are being adhered to. It prevents ambiguities and provides clarity about the laws and their punishments. The key elements of enforcement mechanisms are:

a. Defining the various offences is crucial in order to determine what is punishable and what is not punishable. It provides clarity about what is permitted and acceptable under the SEBI guidelines. Not only does this serve as a standard of appropriate conduct for the advisors, but also makes the investors more aware about their rights and obligations.

b. Determining penalties involves setting a standard penalty for each of the various offences previously defined. This prevents the offender from receiving a penalty that is disproportionate to the offence committed by them. The penalties can be in the form of fines or imprisonment or both.

c. It is necessary to create a body that has the power to penalise persons who do not comply with the regulations and execute the sanctions for the same. An authority must be established to impose punishments on individuals who have failed to comply with the laws and rules.

5. Public awareness campaign- Public awareness campaigns must seek to educate individuals, particularly retail investors and financial advice consumers, on the risks and challenges of following finfluencers. Investors can learn to distinguish between credible and non-credible financial advice sources.

Public education initiatives can also encourage people to do their due diligence before following or acting on a finfluencer's recommendations, educate investors about the regulatory framework that governs finfluencers, the consequences of non-compliance, and inform people about where they can report unethical behaviour by finfluencers.

6.Whistleblower Protection- Whistleblower protection is a crucial part of regulating finance influencers, because it encourages those who have knowledge of unethical or fraudulent behaviour by finfluencers to come forward and reveal the misconduct without fear of punishment.

To safeguard whistleblowers' safety and security, regulatory bodies should provide systems that allow persons to report misconduct anonymously, if they so desire. Furthermore, rigorous confidentiality procedures should be in place to protect the whistleblower's identity.

The fear of reprisal from the individuals or entities being disclosed is one of the key worries for potential whistleblowers. Robust whistleblower protection should include legal provisions to protect whistleblowers from any adverse actions that occur as a result of their revelations, such as job loss, harassment, or legal consequences. Regulatory agencies should create user-friendly reporting mechanisms for whistleblowers. Dedicated hotlines, internet reporting portals, or direct communication with regulatory staff may be deployed.

VII. Conclusion

With the growth of social media, the ecosystem of influencers has grown exponentially over the past few years. Specifically, the internet has experienced a boom in "finfluencers" during the COVID-19 pandemic. However, since there is no legal framework that governs these finfluencers, cases of fraud and misconduct is rampant. The consultation paper issued by SEBI on 25th August, 2023 is a bold step in the right direction. The paper attempts to bring about a legal framework to govern this class of new age advisors. One of the key changes proposed by the paper is to mandate registration of such finfluencers in order to be associated with any registered entity. SEBI seeks to increase transparency and reduce fraudulent activities that are prevalent in the market.

Based on the Indian market experiences, although regulations alone may not completely address the issue of unethical finfluencers, especially in the context of rapidly evolving technology, a potential solution lies in fostering regulated collaborations between registered investment advisors and finfluencers. PR Sundar's case highlights the need the for licensing and mandatory registration with SEBI. However, relying solely on licensing or registration requirements may not adequately address the complexities of this issue. Collaborations between registered investment advisors and finfluencers can be mutually beneficial while also enhancing investor awareness and safeguarding them from potential risks. It is suggested that SEBI should consider establishing a supportive regulatory framework where finfluencers can continue operating while making voluntary online disclosures in real-time, which are accessible to SEBI or a SEBI-appointed monitoring agency. These disclosures should be accompanied by assurances, facilitated through technology platforms, confirming that the finfluencer has no conflicts of interest in providing the advice or recommendations. Any misrepresentations in these disclosures or assurances should result in significant penalties, encompassing not only ill-gotten gains by the

finfluencers and their collaborators, but also losses incurred by retail shareholders and investors. This kind of disclosure can help prevent "pump and dump" schemes such as what happened in the Arshad Warsi case where the prices of a stock was pumped by making false representations in order to attain personal gains.[21]

Although, in accordance with the "*Guidelines for Influencer Advertising in Digital Media*" issued by the Advertising Standards Council of India (ASCI), financial influencers are mandated to include a disclosure label on any content that features financial service companies as an advertisement, there is still a need for far more rigorous measures in order to effectively curb such malpractices.

The struggle between finfluencers and SEBI is about striking the proper regulatory balance that allows financial influencers to thrive while protecting investor interests. SEBI's goal should be to encourage a completely free environment for financial influencers while holding them accountable when their content influences big trading decisions and they profit from it. Recognising the importance of finfluencers in promoting financial literacy is crucial, but so is guaranteeing transparency and ethical practices.

In conclusion, the effective regulation of finance influencers, involves a multifaceted approach that encompasses several key strategies, as proposed by the authors, which are Content Review and Approval, Continuous Education, Establishing a Complaint Mechanism, Enforcement Mechanisms, Public Awareness Campaigns and Whistleblower Protection. By implementing these strategies, regulators can create a regulatory framework that not only curbs potential misconduct but also promotes responsible financial advice and protects the interests of retail investors. Such a framework ensures the integrity of financial markets while enabling the public to access reliable and accountable financial information.

[21] *Why SEBI barred actor Arshad Warsi and others from the securities market*, The Indian Express, (March 4, 2023), Why SEBI barred actor Arshad Warsi and others from the securities market | Explained News - The Indian Express

BLOCKCHAIN TECHNOLOGY AND ITS POTENTIAL TO REVOLUTIONIZE CONTRACT LAW

- ***Suryansh Shukla***[1]

Abstract

This paper comprises various aspects of blockchain technology in legal fields and specifically contract law. Technology is spreading in all the sectors of society and law is not an exception anymore, the obtrusion of it in the legal arena is inevitable. Legal profession is an ever evolving field, new add-ons always bring new challenges and reforms. Specifically, this paper aims to initiate a discussion regarding how blockchain technology and smart contracts can aid legal scholars, dispute redressal structures and completely stir-up the domain of contract law. Blockchain consists of the potential to radically convert the way organisations do business by providing new infrastructure on which the new generation of well-organised business applications will be generated. The potential and ramifications of this technology are so great that they could completely alter how we conduct business today. Instead of taking days, financial firms may settle securities immediately. Commercial contracts might be managed by businesses, making them digital, shareable, and tamper-evident. International best practices from laws such as the United Nations Convention on Contracts for the International Sale of Goods (CISG) can help India streamline its contract system. Implementing unambiguous, standardized language, digital signatures, and worldwide dispute resolution procedures will improve uniformity and efficiency in Indian contract law. Finally, the major aspects of this paper will be its reliance on "off-chain" resources, automated nature, amendment-termination, copyrights and risk factors. Addressing these concerns would confirm blockchain's transformational influence on Indian contract law.

Keywords: *Blockchain Technology, CISG, Smart Contracts, Database, Crypto Currency.*

[1] 2nd Year, BBA.,LLB., Indian Institute of Management, Rohtak. Gmail: suryanshshukla252@gmail.com

I. Introduction

In 2008, Satoshi Nakamoto described how peer-to-peer payments may be made without the need for a centralized infrastructure.[2] There are now more than 1600 distinct crypto currencies available over the market for virtual currencies. The way crypto currencies are growing is rapidly evolving. Being the first, Bitcoin also gained the majority of the market share. The original Bitcoin transaction system is where the notion of block chain technology originated. A blockchain is an electronic ledger that records transactions and makes them publicly accessible when nodes verify them. This picture illustrates the fundamental architecture of blockchain technology. Every transaction is protected by a cryptographic hash function and is verified by the nodes. A transaction that has been uploaded to the blockchain cannot be removed or altered, but it can be publicly seen, adding transparency to the system.[3]

Blockchain validates the transaction using a combination of proof of stake, proof of work, and proof of concept. Blockchain technology is a given away, decentralised ledger system that keeps transaction records transparent and unchangeable. Because, it runs on a peer-to-peer network and each member has a copy of the ledger, there is an extreme degree of security and trust. Because of the immutability of blockchain technology, a transaction once recorded cannot be changed or removed. This feature complies with the Indian Contract Act's requirement that some kinds of contracts be in writing. As, the contract is unchangeable, the parties can have faith in its integrity. The blockchain allows parties to a contract to be authenticated by digital signatures. They can be utilised to satisfy the *Indian Contract Act's* need for free and informed consent by serving as identification and consent proof during the contract formation process.[4]

A computer programme with tamper-resistant, self-executing, and self-verifying features is called a smart contract. "*Nick Szabo"* first put out the idea of a smart contract in the year 1994. It permits code to be executed independently of third parties. The value, address, functions, and state make up a smart contract.

It performs the necessary code, using the transaction as an input, and sets off the output events. Changes in logic implementation states are dependent on the functions with the 2008 launch of

[2] Nakamoto Satoshi, "*Bitcoin: A peer-to-peer Electronic Cash System"* (2008).
[3]Bhabendu Kumar Mohanta, et.al, *An Overview of Smart Contract and use cases in Blockchain Technology*,RESEARCH GATE, 2 (2018).
[4]*Id.* at 5.

blockchain technology via the Bitcoin crypto currency. As, the smart contract integration of blockchain technology allows for peer-to-peer transactions and safe public database maintenance in a trustworthy environment, it is important and should be developed further. Smart contracts include irreversible and trackable features.

Because the term "smart contracts" is used to explain two very distinct concepts, addressing them can be challenging. The prior entails the formation and deployment of smart contracts apart from any supporting text-based contract that is enforceable. As an illustration, two parties may agree verbally on the business relationship they wish to document before directly translating their agreement into executable code. They will be referred to as "code-only smart contracts" from now on. The second one entails using smart contracts as tools to take out specific clauses of a conventional text-oriented contract; the text of the contract itself even makes reference to using the smart contract to carry out specific clauses. These are what we refer to as "ancillary smart contracts."[5]

The concept of "Ricardian Contracts", first proposed by the two scholars *"Ian Grigg and Gary Howland"* in 1996 as a by-product of the research on the Ricardo payment system for asset transfers,[6] is also where modern smart contracts got their start. A single document that Grigg believed to be acting as a link between text contracts and code satisfied the following requirements:

1. A contract that an issuer makes available to holders

2. An important right that holders own and manage

3. Readable by programmes

4. Digitally signed

6. Carries the keys and safeguard the information

[5]Stuart D. Levi, Alex B. Lipton, "*An Introduction to Smart Contracts and their potential and Inherent limitation"*, 19 HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE, 2 (2018).

[6] B. Willi & M. A. I., "*From digital currencies to digital finance: the case for a smart financial contract standard"* 19 THE JOURNAL OF RISK FINANCE, 76-92 (2018).

7. Allied with a unique and secure identifier.[7]

1. Practical Applications of Blockchain Technology

a. Supply Chain

The many transaction levels make up the supply chain management system. Every level has a set of terms and conditions. The supply chain system involves several interconnected systems. The several supply chain system sectors, such as the transportation, food processing, and cargo sectors. A trade is entered into the blockchain database. Improving the transparency of supply chains through the utilization of smart contracts is facilitating the flow in commodities and re-establishing trade confidence.

b. Internet of Things

According to "*CISCO* research", there are currently more Internet of Things (IoT) devices connected to different applications than there are people on the earth. One of the most fascinating areas of research is the IoT. These devices have smaller processor and memory capacities due to resource constraints.

Literature Review

Smart contracts, which are blockchain-powered self-executing contracts, have the potential to completely transform the way that contract law is practised today. This review of the literature critically looks at studies on the legal ramifications and features of blockchain technology in contract law. The research paper by Elena Anatolyevna Kirillova and Varvara Vladimirovna Bogdan titled "Legal Status of Smart Contracts: Features, Role, Significance" is a comprehensive examination of the legal aspects surrounding smart contracts. It offers insightful information about the characteristics, legal standing, and crucial role that smart contracts play in the current contractual environment. The article highlights the importance of these self-executing agreements within the current legal framework while deftly navigating the nuances of these agreements.

Bhabhendu Kumar Mohanta's paper, "An Overview of Smart Contract and Use Cases in Blockchain Technology," offers an insightful exploration of smart contracts and their diverse applications within blockchain technology. The study successfully illustrates the enormous

[7] Stuart, *supra* note 4, at 6.

potential of smart contracts to transform and simplify conventional contractual procedures by painstakingly describing use cases across a range of industries.

Giusella Finocchiaro and Chantal Bomprezzi's work, "A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts," contributes a critical legal perspective on the formation of smart legal contracts using blockchain technology. While carefully examining the legality and consequences of these contracts, the paper also highlights the future legal obstacles in this rapidly changing field.

Zaleha Fauziah, Haznah Latifah, Xavier Omar, Alfiah Khoirunisa, and Shofiyul Millah conduct a systematic review in their paper, "Application of Blockchain Technology in Smart Contracts: A Systematic Literature Review," which successfully synthesises the body of knowledge already known in the field. For those interested in a deeper understanding of the topic, this paper offers an extensive and comprehensive perspective on the use of blockchain technology in smart contracts.

"Smart Contracts – How Will Blockchain Technology Affect Contractual Practices" by Kristian Lauslahti, Juri Mattila, and Timo Seppälä thoughtfully explores the transformative potential of blockchain technology on traditional contractual practices. This paper explores how smart contracts may reshape the execution, administration, and enforcement of contracts in the digital age, posing relevant questions about how the legal landscape is evolving.

"Legal Aspects and Emerging Risks in the Use of Smart Contracts Based on Blockchain," a research paper by Yeray Mezquita, Diego Valdeolmillos, Alfonso González-Briones, Javier Prieto, and Juan Manuel Corchado, offers a critical analysis of the legal aspects and emerging risks related to smart contracts in the context of blockchain technology. This disruptive technology presents both challenges and risks for the legal landscape, which is constantly changing. It provides crucial insights into the legal aspects of contracts based on blockchain.

A thoughtful examination of how well smart contracts work with current legal frameworks can be found in Jelena Madir's paper, "Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?". Madir examines the degree to which smart contracts can be integrated with conventional contract law, tackling essential inquiries regarding their compliance and

enforceability. The paper provides an insightful viewpoint on how disruptive technological innovations and conventional legal frameworks can coexist.

When considered collectively, these research papers show how blockchain technology and smart contracts can transform the practise of contract law, highlighting the need for an adaptable and comprehensive legal framework to address the constantly shifting opportunities and obstacles.

Research Methodology

This research aims to investigate the potent of blockchain technology in revolutionizing contract law, with a certain specific focus on smart contracts. Using a multifaceted research methodology, comprehensive insights into this dynamic and developing field are obtained.

In-depth interviews with legal experts served as the main source of information. Interviews were held with Akshay Sharma, an LL.M. graduate from NLSIU Bangalore and lecturer at IIM Rohtak. We anticipate that Sharma's insights on contract law and block chain technology from an educational and legal perspective will be priceless. Interviews were also held with attorneys, such as Advocate Rahul Singh (Sreeram Finance Limited) and Advocate Abhay Pratap (District and Session Court, Sitapur). The purpose of these interviews was to gather real-world knowledge about the potential and difficulties associated with using smart contracts and blockchain technology in the legal field.

With a focus on historical and judicial viewpoints, the doctrinal approach was utilised to comprehend the implications of various laws related to Smart Contract and Blockchain Technology, while non-doctrinal methods were employed as a secondary source of literature. The project's foundation will be aided by the literature review.

Statement of Problems

1. What will be the impact of blockchain on contract law and its transformative potential if it gets applicable in India?

2. What are the international best practices with respect to Contract under *"International Legislature"* that can be used to simplify the Indian Contract system?

3. What are the issues of legal recognition, privacy concerns and smart contracts vulnerabilities?

II. Smart Contract from the Viewpoint of Contract Law

1. Offer and Acceptance

An offer and an accompanying acceptance are often necessary for the parties to reach the understanding needed to create a legally binding contract.[8] Certain commentators have noted that the uploading of a smart contract to the blockchain by a party is equivalent to making an offer.[9] The offer ought to have every component that makes a contract enforceable. If not, the opposing party is invited to engage in discussions rather than receiving an offer. Durovic and Janssen believe that in this case, the "offeror" publishes his "contract" onto the blockchain in the form of a binary computer code that details the exact parameters of the transaction, and that this would typically be seen as an offer rather than an invitation to treat.[10]

An offer may be made to one or more particular individuals. As an alternative, it might be a suggestion made to the whole public. This relies on the ability of one or more parties to communicate with the smart contract code on a blockchain. More precisely, and from a technical perspective, the offer is made to a particular blockchain user if the smart contract's functions are limited to a certain address (or wallet, or user profile) in the network. In contrast, any user of the blockchain is able to send transactions, making the offer available to everyone.[11]

Regarding acceptance, other than the offeree's consent to the terms of the offer, it need not satisfy any special conditions. As a result, the offeree may accept the smart contract by using a private key to sign a transaction once the offeror has uploaded it. When it is implied by the offeree's actions, acceptance might also take place without a formal announcement. In other words, the offeree's conduct might be seen as a legitimate acceptance of the offer if she begins to carry out the terms of the contract. The offeree must act in a way that is unequivocally indicative of acceptance. For instance, on a blockchain, giving over ownership of a certain sum of money to the code might be regarded as acceptance.[12]

---

[8] J.M. SMITHS, CONTRACT LAW-A-COMPARATIVE INTRODUCTION, (41 NORTHAMPTON, 2017).
[9]Giusella Finocchiaro & Chantal Bomprezzi, *A legal analysis of the use of blockchain technology for the formation of smart legal contracts*, SAGGI, 117-119 (2020).
[10]*Id.* at 8.
[11] J. Earls et al., *Smart Contracts, Social Science Research Network* (SSRN, 2019).
[12]M. Raskin, *The Law and Legality of Smart Contracts*, GEORGETOWN LAW TECHNOLOGY REVIEW 322 (2017).

2. Consideration

An English court will probably take mutual benefit and burden into account when determining whether a smart contract is supported by consideration. Courts in Australia and England won't challenge whether anything has been accorded "adequate" value. Similarly, anything of value, even minuscule amounts exchanged between the parties, is typically considered under US law.[13]

3. Contractual Intention

The status of the party's communications with one another is analyzed by the relations to what was delivered between the parties by words per se or conduct, and whether that leads objectively to an end result that[14] the parties intended to create legal relations. This is how the parties intentions are evaluated under English, US, and Australian laws.

"*It may therefore be challenging for a party to assert against the other party that relied on the smart contract that there was no intention to establish legal relations with regard to the smart contract if the other conditions for a legally binding contract are met in the case of a smart contract*." Smart contracts have the ability to act proactively, which is one of their main advantages.

For instance, if a party has voluntarily entered into a smart contract ("the primary contract"), the primary contract itself has the ability to enter into additional contracts ("the secondary contract"). For instance, banks and lenders could consent on a framework agreement whereby the software automatically sends a loan application to the lender if the borrower's bank balance drops below a pre-specified way, and the loan application is automatically approved if certain pre-programmed conditions are met. This includes establishing new loans on a regular basis (not simply reducing existing loans). Since, the parties first decided to conclude a smart contract, they may argue that they agreed to a system that was implicitly bound by the system in question.[15]

By programming the software to automatically request a loan when the necessary conditions are satisfied, the borrower can be identified as making a conditional offer for the loan (i.e. from the time the borrower's balance touches the relevant way in). Similarly, the lender would accept the

[13]Jelena Madir, *Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?*, SOCIAL SCIENCE RESEARCH NETWORK, (2019).
[14] Herbert Smith Freehills, *The Rocky Road from Letter of Intent to Formal Contract*, GLOBAL LAW FIRM (31 October 2023), <https://www.herbertsmithfreehills.com/insights/2016-12/the-rocky-road-from-letter-of-intent-to-formal-contract>.
[15]*Id*. at 10.

offer on conditional terms by automatically accepting any loan application that meets pre-programmed conditions by coding a software.[16] The smart contract certainly generates the loan request and acceptance communication when these conditions are fulfilled, which leads to a new loan contract.

"Section 10 of the Indian Contract Act, 1872",[17] stipulates that all contracts must be written or expressed in such a language that is endorsed by the parties, and signed by the parties concerned. Smart contracts are not traditional contracts, but are considered in accordance with this paragraph. The code that forms the smart contract is a written contract, the terms of which are usually expressed in the programming language understood by the parties. In addition, blockchain records the transactions and provide digital signatures that verify the authenticity of contracts.

4. Formation of Legally Binding Contracts

The fundamental idea behind smart contracts is that they enable the programming of agreements between parties. This status of the programming suggests that there is a mechanism to have an agreement fulfilled automatically and that it is not left up to interpretation. In this regard, a programmer's job is essential to translate a legal agreement's clauses into code.[18]

Because of the difficulties that result from the law's imprecise interpretation, a programmer may require legal counsel. A legal entity must communicate to the programmer and the representation of each legislation's clause in order to create a well-translated smart contract that takes into consideration the interpretation of any laws that may have an impact on it. The Spanish Civil Code's 1256 article, which states that "the validity and performance of contracts cannot be left to the free will of one of the contracting parties," is fulfilled by the very nature of the Smart contracts implemented by blockchain technology.[19] In India, a similar provision is there in the Indian Contract Act of 1872. Specifically, section 4 of the Indian Contract Act 1872[20] regulates the manner of communication of acceptance. It states that the acceptance of communication is complete as against to the proposer when it is placed in the process of the communication to him

[16]RTS Flexible Systems Ltd v. Molkerei Alois Müller GmbH & Co, *KG* (2010) UKSC 14.
[17] Indian Contract Act, 1872, § 10, No. 9, Acts of Parliament, 1872 (India).
[18] Yeray Mezquita, et.al, *Legal Aspects and Emerging Risks in the Use of Smart Contracts Based on Blockchain*, SPRINGER NATURE SWITZERLAND, (2019).
[19]*Id.* at 11.
[20] Indian Contract Act, 1872, § 4, No. 9, Acts of Parliament, 1872 (India).

so as not to be under the authority of the acceptor. It is similar in spirit to Article 1256 of the Spanish Civil Code in that it deals with the method of communication and the time at which the acceptance becomes effective.

Another foundation for the implementation of *"smart contracts"* is found in article 1281 of the Civil Code of the said law, which states that *"If the terms of a contract are clear and leave no doubt as to the intention of the contracting parties, it is in the literal sense of its clauses."* This means that the parties that consented to the terms of the contract are aware of them and do not need to interpret them.

Once again, the similar pattern can be traced in Indian context as according to contract law, the language used in a contract must make it obvious what the parties intend, and it must contain clear and precise terms. A smart contract must be precise, unambiguous, and devoid of any space for interpretation or uncertainty about the parties intentions in order to be deemed legitimate and effective under Indian law. A contract's ambiguity may give rise to disagreements and legal problems.

Conventional contracts are susceptible to breach and rely on human intervention for performance. Contracts with smarts are automated. Whether the Act's principles should be applied is the main concern. Another very important question arises here regarding the management of disputes and enforcement as most often the parties are international as well as sometimes pseudonymous. Adding on to it, Indian Law is a centralised legal system, but blockchain technology is decentralised.

5. Liability

Such intricate relationships give rise to a variety of problems and considerations: "*First, the ownership of the distributed ledger software code is probably a matter of property or copyright law, and the answer could have an impact on who bears liability for the code in terms of tort law.Secondly, a third party may attempt to apply a tort law claim against all nodes jointly if it suffers harm due to a security breach or coding error."*[21] This is unlikely to succeed because proceedings and actions can only be taken against a (legal) body and not regarding a "*node"* or, more broadly, a method. In cases of negligence, a party's liability is generally determined by

[21] Jelena, *supra* note at 13, 9.

three factors: whether the party had a duty of care, which was breached, whether the breach resulted in loss or damage, and whether the party effectively waived its liability for this kind of loss or damage in the contract.[22]

The handling of the cooperation that underpins a distributed ledger is another problem. For instance, who among the numerous nodes (if anyone) is legally accountable for system hacks, and are those who collaborate in a system liable for failures?[23]

"Smart contract templates should for preference include a space for indicating the contracting parties choice of liability scheme in the event of a coding error, to encourage parties to at least think about the allocation of liability." Parties would still be able to choose to use no liability allocation mechanism, though. In this situation, "an automated warning message might be sent to the parties informing them that failure to designate a liability mechanism could result in the allocation of losses wherever they fall and asking them to confirm that they do not wish to specify what should happen in the event that the code deviates from their expressed written wishes."

Furthermore, there exist numerous potential non-contractual liabilities that could emerge in connection with specific transactions executed via smart contracts. These liabilities could include, but are not limited to, allegations of fraud, unfair trade practises, insider trading, market manipulation, etc.[24] Insurance companies may be able to cover liability risks in relation to smart contracts by filling in the liability gaps. Drafting the terms under which such insurance is applicable will be extremely difficult.

6. Burden of Proof

Each party must present its own claims in court and file an application for legal enforcement with the appropriate court in many jurisdictions due to applicable procedural rules. Generally speaking, a claimant assumes the risk that the facts it is relying upon cannot be proven and must frequently prove them. For instance, If Party A does not make a payment according to a non-smart contract that requires Party A to make a contribution to Party B, Party B would generally

[22] *Hedley Byrne & Co Ltd v Heller & Partners Ltd*, (1964) AC 465.
[23] Jelena, *supra* note at 13, 9.
[24] *Id.* at 12.

have to claim and prove in court that it is entitled to a legitimate payment claim and that Party A has not paid.

"Party B would also need to apply to the court for the legal enforcement of a judgement determining that Party B has a valid claim for payment if Party A continued to withhold payment." Therefore, Party B would bear the risk of both Party A declaring bankruptcy before the judgement is legally enforced and the legal risk that Party B is unable to support its claims. These broad principles also apply to claims involving smart contracts; however, due to automation, the specifics of the claim, including the burden of proof and associated risks, will almost certainly change. In the example given, "*Party B would automatically receive payment and would not be required to pursue its payment claim in court*." On the other hand, Contractor A would now need to pursue and, in most cases, prove its claim for reimbursement of the appropriate amount if it believes that the payment was not made correctly. This would result in Contractor A having to bear the legal burden of proving its claim, as well as the risk of Contractor B succumbing to insolvency prior to the repayment. Furthermore, Contractor B may also face other legal consequences, such as a lack of ability to exercise retention and set-off rights, both within and outside of litigation.

Contracts with anonymous third parties are more likely to be signed by Party B, who stands to gain from this procedural reversal and shift of risk. But, not every situation calls for this "reversible" and "shift" of risk that comes with a contract being automatically executed. For instance, some kind of parties ("consumers") may not be able to take on this generated risk. Therefore, some legal systems may seek to stop any variation of the normal burden of proof against a consumer.[25]

III. With Smart Contracts

1. Privacy Issues

Privacy is concerned with the safeguarding of personal data, which is information that can be directly or indirectly linked to a living individual. This may include personal information such as name, address and telephone number, but may also include a collection of other information that

[25] Smart Contracts: Legal Framework and Proposed Guidelines for Lawmakers, Clifford Chance (October, 2018),https://www.ebrd.com/documents/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf?shem=ssusba.

collectively has something to do with an identifiable individual. For example, location information or video footage may be considered personal data if incorporated into a distributed ledger. Under the "European Union's General Data Protection Regulation (GDPR) 2016/679", citizens have a range of rights regarding their personal information, including the right to rectify personal information, erase it and forget it. In the context of smart contracts, data has been pseudonymised, rather than anonymised, thus remaining personal data for the purposes of the GDPR.

The GDPR makes a distinction between data processors and controllers. A data controller is an individual who chooses how and why to process personal data; a processor merely handles personal data on the controller's behalf. It can be difficult to identify these individuals and their roles, especially in light of the non-centralised nature of permission less "*Distributed ledger technology -based systems (DLT)"* and the strength of network users to engage in direct smart contracts, share resources peer-to-peer, and add data to the ledger without needing permission from a core administrator.[26]

Instead of directly logging specific data in a blockchain, it is frequently used to incorporate hyperlinks into a blockchain that can be connected to lines containing specific data. This does not change the fact that specific data is being reused, even though it makes it simpler to remove or modify specific data (see below). Thus, the question of whether the GDPR applies to a blockchain where specific data is reused is determined by whether processing takes place in the context of conditioning an establishment of one of the regulators in the *European Union*, rather than by whether there are bumps located within the EU. Acknowledging this difficulty, the European Parliament has requested additional guidance on how blockchain-based operations can comply with the GDPR from the *European Commission* and the *European Data Protection Supervisor*.

2. Dispute Resolution Mechanism

In the complex world of smart contracts, where automated deals do across distributed computing systems, the determination of governance and applicable governing law poses a significant challenge for courts. Smart contracts tone- executing nature makes it delicate to pinpoint the

[26] Jelena, *supra* note at 13, 9.

place of performance, leaving courts in a double bind when deciding which legal frame should apply to controversies arising from these contracts. Despite these challenges, courts won't wince down from taking governance over smart contract controversies, but the query prevails regarding which court will step by and which governing law it'll apply. Still, there's a hint of stopgap in navigating this jurisdictional maze. Courts are not non-natives to resolving jurisdictional issues, similar as those arising from contracts formed over the internet, like online purchases of goods and services.

To address the jurisdictional inscrutability associated with smart contracts, it's suggested that an obligatory field within the smart contract be included, allowing the parties to indicate their choice of governing law. In numerous authorities, courts will generally uphold the parties' unequivocal choice of law to the topmost extent possible. Parties should take care to elect a governing law that recognizes contracts written in law, concluded electronically, or with pseudonymous counterparties as fairly binding. Nonetheless, a pivotal issue looms concerning the position of the smart contract.

This determination is vital in catching on which professional nonsupervisory or taxation governance should be applied, and it may not always align with the parties' agreement. Rather, it frequently involves an objective assessment grounded on the place of performance. In cases where conflicts of law rules mandate that, in the absence of an express choice of law, the applicable law is that of the governance where an asset is located, a practical consideration arises concerning native means on permission less blockchains. Native means on a public blockchain, much like trade secrets or unrecorded imprints, warrant a central depository or enrolment authority. To alleviate this, parties to smart contracts might conclude to share in a permissioned blockchain with a centralized authority or use a third-party conciliator, similar as an estimable portmanteau provider, to hold blockchain grounded means.

This approach provides further certainty that these means are located in the governance where the central authority or third- party conciliator operates. Still, it comes at the cost of decentralization, an abercedarian principle cherished by numerous blockchain lawyers. In summary, the complications of governance and governing law in smart contract controversies are indeed grueling, but not invincible. Parties can enhance pungency by expressly designating the governing law within the contract, while also considering the practical counter accusations of

where the smart contract is executed. As smart contract technology continues to evolve, legal fabrics will need to acclimatize, but for now, careful consideration of these jurisdictional and legal issues is vital for parties engaging in smart contract deals.

In 2020 Supreme Court of Canada ruling in *Uber Technologies Inc v Heller*[27], the court considered the legitimacy of an arbitration provision that required disagreements to be addressed in the Netherlands, with significant upfront payments. Heller, a food delivery driver, said the condition was unconscionable because of the huge power imbalance and financial burden. The Supreme Court agreed with Heller, deeming the clause unconscionable due to the imbalance of negotiating power and the improvident language. This case emphasizes the necessity of fair contract terms, as well as the potential role of blockchain technology in guaranteeing equal and transparent contract enforcement.

Scope for further Research

1. How are smart contracts negotiated, drafted, and decided by non-technical parties?

Parties to smart contracts will need to rely on a trustworthy third party, which is a major barrier to their widespread adoption, knowledgeable specialists to either bind the parties' agreement to the letter of the law or verify the accuracy of third-party legal writing. The comparison is flawed, despite the fact that some liken this to hiring a legal counsel to interpret "the legalese" of a conventional textbook grounded contract. Most short form agreements and many essentials of longer agreements especially those defining business terms can be understood by non-lawyers. However, even the most basic smart contract would be wholly incomprehensible to a non-programmer, which severely limits their ability to ask an experienced person to interpret the terms of the contract. To some limit, *"the incapability of constricting parties to understand the smart contract law won't be an interference to entering into ancillary law agreements*".

This is because for numerous introductory functions, textbook templates can be created and used to indicate what parameters need to be entered and how those parameters will be executed. *"For illustration, assume a simple smart contract function that excerpts a late figure from counterparty's portmanteau if a set payment isn't entered by a distinct date."* The textbook template could prompt the parties to begin with the quantum of the anticipated payment, the due

[27] Uber Technologies Inc v Heller, (2020) SCC 16.

date and the quantum of the late figure. Still, a party may want to confirm that the underpinning law actually will perform the functions prescribed in the textbook, and that there are absolutely no fresh stipulations or conditions especially where the template disclaims any liability arising from the delicacy of underpinning law.

This inspection will be conducted by an unbiased, experienced programmer. In cases where templates like this one don't exist and new legislation needs to be made, the parties would desire to explain the goal of their agreement to a programmer. Giving the programmer a blank copy of the contract would be problematic because it would require the programmer to attempt to decode a legal set of documents. Therefore, parties relying on "*ancillary smart contracts"* might have to write a separate "term distance" outlining the functions the smart contract is supposed to carry out, which they can then, give to the programmer.

The programmers may also be asked to provide the parties with written assurances that the law operates as intended. As a result, similar to contracts that parties may sign with service providers for *"Electronic Data Interchange"* (EDI) deals, the parties may need to enter into a written agreement with the smart contract programmer for custom designed arrangements that don't compute on an existing template. "*The insurance companies could also create policies to protect parties that are in a restrictive agreement from the possibility that smart contract law fails to fulfil the requirements outlined in an agreement textbook. Insurance can provide additional protection since the parties may overlook crimes when reviewing the law, even though they would also want to review it themselves or have third parties do so."*But, the fact that the insurance company most likely carried out its own legal examination prior to consenting to guarantee compliance with the law would also provide the parties with some newfound comfort. "*Law only smart contracts used for business to consumer deals could pose a fresh set of issues that will desire heeding."*[28]

"Courts are cautious of administering agreements where the consumer didn't admit acceptable notice of the terms of the agreement, and may be reluctant to apply a smart contract where the consumer wasn't also handed with an underpinning textbook agreement that included the complete terms." Eventually, in order to help courts understand the intent and meaning of the law, a system of court-appointed experts may be necessary as the validity and performance of

[28]Stuart, *supra* note 4, at 6.

smart contracts are less frequently arbitrated. at the moment, parties routinely use their own experts when specialized issues are at the centre of a disagreement. *"Although many state courts as well as civil courts possess the ability to designate their own experts, they rarely do so. That strategy might need to alter if the standard contractor's quantity changes controversies that centre on interpreting smart contract law increases."*[29]

Legislation becomes successful only when it is highly accepted and the same goes with the Contract Law as well. If contracts start getting dishonoured, the legislature will definitely start losing its value. People will honour contracts only when they completely understand it and its significance. "Although, till date some solutions have been provided by legal scholars, but it still seems relatively far-fetched for non-technical legal scholars. Hence, there is a need for more development in this arena."

2. How to deal with the automated nature of Smart Contracts under "Indian Contract Act, 1872"?

The ability of smart contracts to apply deals automatically and persistently without the need for human intervention is one of their most important features. However, some of the biggest arguments against the widespread abandonment of smart contracts are this robotization and the fact that they cannot be easily changed or terminated unless the parties incorporate comparable capabilities when creating the smart deal. ("For example, in classic textbook contracts, a party can easily ignore a breach by choosing not to apply the applicable penalties."). If an appraised client is one month overdue on payment, the seller may, nevertheless, decide in real time that maintaining the long-term marketable relationship is more crucial than any reachable limitation of birth right or late figure. Still, if this context had been degraded to a smart deal, the option not to apply the consensus on an ad hoc base probably would not live.

"A delayed transaction will affect the spontaneous birth of a late figure from the client's account or the suspense of a client's access to a piece of software or a gadget with an internet connection if that's what the smart deal was programmed to do."

The automated prosecution handed by smart contracts might thus not align with the manner in which numerous companies go on in the real world.[30]

[29] *Id.* at 19.
[30] Stuart, *supra* note 4, at 6.

"Similar to this, a party to a text-based contract may be prepared to agree upon, on as-needed basis, partial performance in exchange for full performance. This may occur from a desire to maintain a long-term relationship or from a decision that some performance is better than none at all on the part of one of the parties." Once more, the objectivity compulsorily for smart contract coding may not accurately represent the interactions between *"contracting parties"*.

Although, several advancements to cope up with this situation are going on, there is huge scope of improvement for the same. *"One of the most recurring question that still comes in the mind even after some clarifications is; how can the Indian Contract Act of 1872 be updated and modernised to effectively address the issues raised by the automated and self-executing nature of smart contracts, ensuring legal clarity and enforcement in the digital age, given the quick developments in smart contract technology?"*

IV. Suggestions

New kinds of instruments are emerging as a result of digitalization, challenging our conventional knowledge of contracts and their mechanics. Understanding the true nature of these kinds of agreements can be difficult when cooperation is, in extreme circumstances, solely governed by the smart contract's programming code. Despite the fact that this paper has only covered three instances of smart contracts, there could be an almost limitless number of other uses. In certain situations, it is evident that a contract lacks certain necessary components, but in other situations, the requirements for a valid contract are probably always satisfied.

There are many situations in between these two extremes where a smart contract's legal implications will probably depend on how it was completed. Consequently, the issue of who gets to decide when smart contracts written in code are thought to be regarded as legal contracts in some, but not all situations naturally comes up. "*An important question from the perspective of legislation is which public entity has or should have the technical skills and capacity to analysethe legal character of smart contracts on a case-by-case or larger-scale basis, given the lack of a model for classification or case law at this time*."[31]

Should each case of a smart contract be considered separately in court to determine its validity? Conversely, is it feasible for government or public organisations to assume accountability for

[31] Kristian Lauslahti& Timo Seppalai, *Smart Contracts – How will Blockchain Technology Affect Contractual Practices?*, ETLA REPORT IT, 86 (2017).

elucidating the legal standing of smart contracts?[32] In response, one may wonder if the various industries ought to take preventative action and draught sample contract clauses that encourage the use of smart contracts.

"The techno-economic point of view has historically been chosen as the primary framework for comprehending a variety of phenomena and their effects when looking at technological disruptions." Lately, there has been a growing recognition that legal regulation plays a significant role in the advancement of innovations. Additionally, reality has demonstrated that, in the case of the platform economy, techno-economic anticipation alone has not always resulted in functional regulatory practise. For example, the need for new regulations targeted at the appropriate subjects has arisen due to the new business model that has gained recognition since 2007 and served as the foundation for services like Uber. It is now insufficient to merely be aware of the technologies being developed in the current environment; one must also comprehend their effects.

Therefore, it is reasonable to assume that blockchain technology will impede the growth of the platform economy by, for instance, opening up previously unheard-of channels for collaboration and communication and by introducing novel techniques for technical contracting. Although, blockchain technology is still in its early stages of development, several technology suppliers estimate that it will be ready for the development of large-scale applications in about 2.5 years. Thus, from the perspective of the legislator, now would be the ideal time to comprehend blockchain technology and come to terms along its implications while research into this novel technology is still being conducted.

V. Suggested Consideration for Legislators

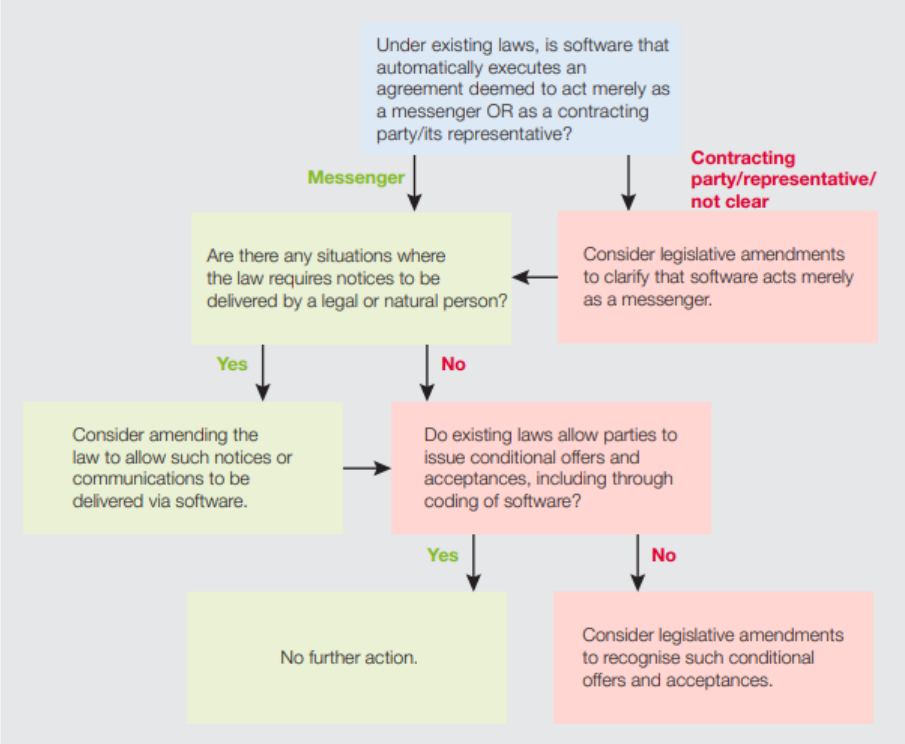
Legislators must first determine whether software, under the terms of the law, automatically executes agreements (as long as certain requirements are met) is merely acting as a messenger for the applicable parties to the agreement, or if it may be construed as acting on behalf of the contracting parties themselves (or as their agent or representative). *"Legislators may want to*

[32] *Id.* at 19.

think about changing relevant laws to make it clear that software only serves as a messenger or medium of communication in this situation if the current laws do not offer a clear solution."

Legislators should also determine whether the current legal framework permits contracting parties to make conditional offers and acceptances, even through automated software (which is frequently the case when parties use the Conclusion Model to enter into smart contracts). If not, lawmakers might want to think about changing current laws to make it easier to use smart contracts under the Concluding Model. For instance, they could recognise the parties actions when coding software automatically concludes a contract when certain conditions are met, such as when an offer is made and accepted conditionally.[33]

Lastly, legislators should determine if there are any circumstances under which a legal entity must issue notices or other communications pertaining to contracts. If this is the case, legislators should think about amending current laws to permit the delivery of such notices or communications via software in the context of a smart contract.



[34]

[33] Clifford Chance, *supra* note at 14.
[34] *Id*. at 20.

VI. Conclusion

Considering the field of blockchain technology and its significant impact on contract law, we must handle this issue with the utmost gravity, accuracy, and discernment. We must embrace innovation with caution in the dynamic landscape of the digital age, where transactions happen with unprecedented speed and autonomy. As a decentralised ledger of unchangeable records, blockchain technology upends the preconceived ideas ingrained in contract law. As we consider the implications of smart contracts self-executing agreements that function outside the purview of conventional contract interpretation this transformative force requires our undivided attention. Several legal scholars have taken a nuanced approach, emphasising the need to protect the sanctity of contractual relations. Blockchain's cryptographic foundations provide a ray of hope in a world where trust is frequently hard to come by, possibly increasing trust in contracts and making them more safe and dependable. However, the need to protect the fundamental principles of contract law cannot be overstated.

It is impossible to overestimate how disruptive blockchain technology could be for contract law. It's a challenge that goes beyond conventional legal paradigms and calls for a careful and thorough response. Maintaining the fundamentals of contract law while embracing innovation and modernising for the digital era all require a delicate balance. Remember that the law is a mirror of our changing society and must adapt along with it, aided by the insight of our legal elites, as we forge ahead into this uncharted territory.

THE CLOUD TRIAD: TECH, LAW, AND TOMORROW

- ***Kotha Nitin Bhargav &Goduguluri Venkata Sri Vidya***[1]

Abstract

This article delves into the multifaceted realm of cloud computing, offering a comprehensive exploration of its technical intricacies including its parameters and deployment models, cloud-based services, techno-legal challenges, and the promising horizons that lie ahead. The technical aspects unravel the core functionalities and innovations driving cloud technology, providing insights into its dynamic and evolving nature through its service models. Simultaneously, the discussion on techno-legal challenges sheds light on the legal complexities and regulatory considerations surrounding cloud computing, addressing the intersection of technology and the law. Looking toward the future, the article outlines emerging trends and potential advancements that could reshape the landscape of cloud computing. Together, these components provide a holistic view, guiding readers through the present complexities while offering a glimpse into the fascinating possibilities on the horizon in this techno-legal world.

Keywords*: Cloud Computing, Cloud Security, Hybrid Cloud, Data Privacy, Utility Computing.*

[1] 5th Year, B.A., LL.B., DamodaramSanjivayya National Law University. Gmail: nitinbhargav2002@gmail.com&godugulurisrividya@gmail.com

I. Introduction

In the intricate tapestry of technological evolution, few innovations have had as profound an impact as cloud computing. The roots of this transformative paradigm extend back to the conceptualization of utility computing, where computing resources were envisioned as a service akin to electricity. As we trace the historical trajectory, we encounter milestones such as the paradigm-shifting advent of Virtualization, a technological cornerstone that paved the way for the scalable and flexible infrastructure characteristic of modern cloud environments. Concurrently, the rise of Web 2.0 introduced a collaborative and interactive dimension, further shaping the landscape that would become the bedrock of contemporary cloud computing.

However, understanding the essence of cloud computing goes beyond its historical roots. At its core lies a sophisticated architecture that facilitates the seamless delivery of services over the internet. This architectural prowess is manifested in various deployment models, ranging from public clouds that offer services to multiple clients, to private clouds dedicated to a single organization, and hybrid clouds that amalgamate the strengths of both. The services hosted in these clouds encompass a spectrum of functionalities, from Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) to Software as a Service (SaaS), each contributing to the diverse and interconnected ecosystem that characterizes cloud computing.

Cloud generally refers to the Internet, it presents over the remote location. It provides different network services on public networks or on private networks, i.e., Wide Area Network, Local Area Network or Virtual Private Network. Customer Relationship Management is the best application which runs on the cloud.

A **Computing Cloud** is a set of networks enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way.[2]

This Cloud Computing delivers services on servers, storage, databases, networking, software, analytics, intelligence, and more, over the Cloud (Internet). Cloud Computing offers an alternative to on-premises data centers, as it allows users to rent services from a cloud vendor

[2]Lizhe Wang, Gregor von Laszewski, Et Al., *Cloud Computing: A Perspective Study*, New Generation Comput., SPRINGER LINK, 2010, 28. 137-146. 10.1007/s00354-008-0081-5.

who takes care of hardware purchase, maintenance, and provides various software and platform options, with charges based on usage.

II. Cloud Computing: A Technical Perspective

1. Background and Evolution of the Cloud Computing Technology

Before the computing technology arrived, users depended on server architecture for accessing their data where all the data and control of the client resides on the Server side. This works in such a way that if a single user wants to access the data; firstly, the user needs to connect to the server from where the user gets the appropriate access which involved many disadvantages that led to the arrival of new technology called as distributed computing where all the computers are networked together that helps the user to share their resources when needed. But this technology also had its own implications and limitations that led to the emergence of cloud computing.

Before the evolution of Cloud Computing, many phases had existed in cyberspace for the purpose of accessing the information by the user. Out of these five technologies have played a vital role in making cloud computing what it is today. The first idea originated in the early 1950s. Those technologies are known as distributed systems and their peripherals, virtualization, web 2.0, service orientation, and utility computing.

a. Distribution Systems and its peripherals

These distributed systems are composed of multiple independent systems, appear as single entities to users who aim to share and utilize resources effectively. These systems possess characteristics like concurrency, scalability, availability, heterogeneity, and independence in failures. However, the requirement for all the systems to be present in a single geographical location turned out to be the main problem in this technology, which was later developed into mainframe computing, cluster computing, and grid computing to tackle the problem in distributed systems.

i. Mainframe Computing

These mainframes came into existence in 1951. Here, in mainframe computing all the resources will be located at one central location. To perform any action or function of the user-related activities these resources will be accessed through a terminal. These mainframes are responsible for handling

large data such as massive input-output operations. One of the biggest disadvantages of this mainframe computing is that when the user accesses any of the resources within the mainframe, it will connect to various resources because all these resources are correlated. So, here we cannot retrieve the information easily because of many connections.[3]

ii. Cluster Computing

This is the new technology that was developed after mainframe computing which provides the user an opportunity to access the information and perform any function or action through the various machines which are connected in the form of a cluster that is interlinked to each other through networking with a high bandwidth. Also, it provides the facility that new nodes can be added to the cluster whenever necessary. But still, the geographical location problem still persists which led to the development of new technology known as Grid Computing.[4]

iii. Grid Computing

This technology was evolved to solve the issue of geographical location. And this was solved in a way that enabled the connectivity of many systems through the medium of the internet. In this grid technology, various systems belonging to various organizations will be connected to each other and hence this network consists of heterogeneous nodes. However new issues have been unlocked because of this technology such as the requirement of high bandwidth of the internet in order to connect the various networks in the form of a grid; also, the distance between the nodes is more due to various geographical locations. To tackle this issue cloud computing has emerged.[5]

b. Virtualization

This is the process of creating a virtual layer over the hardware which allows the user to run multiple functions, or actions simultaneously on the hardware. This technology is often used to create Virtual Machines (VMs) that can run different

[3] Henri van Maarseveen, *From Mainframe Computing to the Cloud: The Evolution of SaaS*, KINDLE ED., 10 February 2023.
[4] *Id.*
[5] Zlatanov, Nikola, *The data center evolution from Mainframe to Cloud*, RESEARCH GATE PUBLICATIONS, March 2016.

operating systems (OS) and applications on the same physical hardware. Hardware virtualization is a key technology used in cloud computing, which enables the creation of virtualized infrastructure on top of physical hardware. Hardware virtualization is also used in desktop virtualization, where multiple virtual desktops can be created on a single physical machine.

c. Web 2. o

It is the term used to describe the second generation of the World Wide Web (www) which is the shift from static web pages to most interactive and dynamic webpages which allows the user to collaborate and participate to create the content. Web 2.0 is characterized by the use of social media, user-generated content, and web applications that allow users to interact with each other and with the content on the web. The web interface is the point of interaction between the cloud computing services and the clients. It is how users access and interact with the cloud-based applications and services. Some popular examples of Web 2.0 include Google Maps, Facebook, Twitter, and YouTube. These platforms are characterized by user-generated content.

d. Service Orientation

In the context of cloud computing, a reference model is a blueprint that defines the components and relationships of a cloud computing environment. In this computing model, important concepts were established such as Quality of Service (QoS) which refers to the ability of a cloud service provider to deliver a certain level of performance and reliability to its customers which also includes Service Level Agreement (SLA) which defines the QoS metrics that the service provider will deliver, as well as the consequences if the provider fails to meet those metrics; and Software as a Service (SaaS) which is a model of cloud computing in which software applications are delivered over the internet.

e. Utility Computing

Utility computing is a computing model that provides services on a pay-per-use basis. It is a service provisioning technique that allows users to access computing resources such as computing services, storage, infrastructure, etc. The benefits of this utility computing are Cost savings, Flexibility, Scalability, and Reliability.

However, all the above-mentioned techniques and technologies have contributed to the making of Cloud Computing.

2. Parameters of Cloud Computing

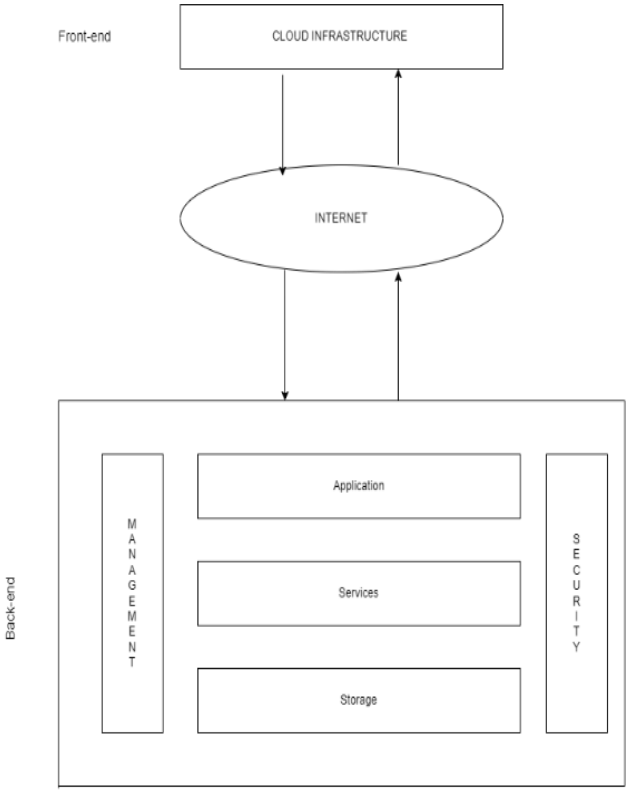
The following are the parameters of cloud computing: -

a. *Global in minutes* - the servers will be deployed in the cloud, which will enable the user to retrieve the data within seconds from that cloud.
b. *Variable v. Capital Expense* - Data will be in virtual machines in the cloud, so there will be no need for capital expenses. While there is a need to spend the operational expenditure for the operations performed by the user like pay-as-you-go when the business is growing well otherwise there is no need to pay the operational expenses as there will be no need for the cloud when the business is low. Within cloud computing, there will be no investment expenses as the hardware, software and other components will be in the control of the other party which is on a rental basis.
c. *Economies of Scale* - Economies of scale in the context of cloud computing refer to the cost advantages that cloud service providers can achieve as they scale their operations and infrastructure to serve a larger number of customers and workloads. These cost advantages arise from the ability to distribute fixed costs over a larger customer base, optimize resource utilization, and make more efficient use of hardware and software resources.
d. *Increasing Speed and Agility* - This is indeed a significant parameter and benefit of cloud computing. Cloud computing provides several features and practices that enable organizations to become more agile and responsive to changing business demands.
e. *Focus on business differentiators* - Due to this cloud computing there will be no spending of time on other things as all the overhead will be looked at by cloud computing, so the user can focus on the business and its expansion.
f. *Stop guessing capacity* - There is no requirement to guess the capacity of the number of data centers required as in the traditional approach (Data Center approach). Here, in cloud computing systems scale up accordingly with respect to the required capacity

for the growth of the business, and even in case there is a decrease in business, automatically systems scale down & servers will be shut down. Only those centers which the user uses as per the required capacity the payment has to be made i.e., pay as you go. This feature of scale up and scale down is available in cloud computing; so, there is no need to have guessing capacity.[6]

3. Cloud Computing Architecture

This cloud computing architecture can be represented in 2 parts. These are Front-End and Back-End which communicate via a network or through the internet. It can be represented as:



Picture -1[7]

FRONT-END: It provides applications and the interfaces that are required for the cloud-based service. It consists of client-side applications, which are web browsers such as Google Chrome and Internet Explorer. Cloud infrastructure consists of hardware and software components such as data storage, server, and virtualization software and also provides a Graphical User Interface to the end-users to perform respective tasks.

BACK-END: It is responsible for monitoring all the programs that run the application on the front end. It has a large number of data storage systems and servers.

a. Cloud Computing Architecture Components

i. Hypervisor - A hypervisor is a software program that creates and manages virtual machines (VMs) on a cloud computing platform. It provides virtual

[6] *Id.*
[7] This flowchart depicts the cloud infrastructure and its components.

operating platforms to every user, which means that each user can have a virtual machine with its operating system. The hypervisor also manages guest operating systems in the cloud, which are the operating systems running on the virtual machines.

ii. Management Software - Management software is responsible for managing and monitoring cloud operations. It uses various strategies to increase the performance of the cloud, such as load balancing, auto-scaling, and resource allocation. The management software also provides tools for monitoring the health and performance of the cloud, such as dashboards and alerts.

iii. Deployment Software - Deployment software is responsible for installing and configuring all the necessary components to run a cloud service. This includes infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS). The deployment software ensures that all the components are installed correctly and configured to work together.

iv. Network - The network connects the front-end and back-end of the cloud computing platform. It allows every user to access cloud resources, such as virtual machines and storage, over the Internet. The network also provides a virtual server that is hosted on the cloud computing platform, which can be accessed by users from anywhere.

v. Cloud Storage - Cloud storage is a scalable storage solution that is automatically accessed by users over the internet. Every bit of data is stored and accessed by a user from anywhere over the internet. Cloud storage is designed to be highly available and fault-tolerant, which means that data is replicated across multiple servers to ensure that it is always accessible.

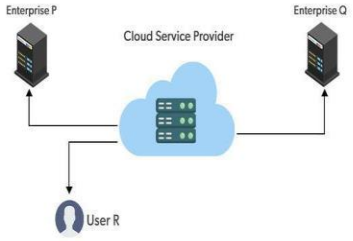
4. Deployment Models

Cloud Deployment Model refers to the way in which cloud computing services are deployed and accessed by users. It is a virtual computing environment that allows users to access computing resources over the internet. The deployment architecture of the cloud deployment model varies depending on the amount of data that needs to be stored and who has access to the infrastructure.

The cloud deployment model determines the ownership, scale, access, nature, and purpose of a cloud environment, including the location and control of servers, and defines the relationship between the infrastructure and users.

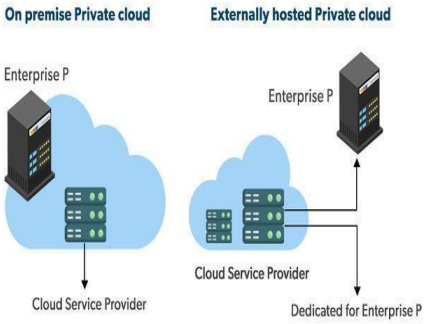
The various types of cloud computing deployment models are public cloud, private cloud, hybrid cloud, and community cloud.

a. *Public Cloud* - The public cloud allows easy access to systems and services, but it may be less secure as it is open to everyone. The infrastructure in this cloud model is owned by the entity that delivers the cloud services, not by the consumer.



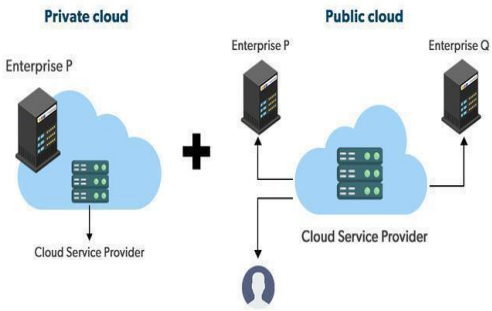
Picture - 2[8]

b. *Private Cloud* - The private cloud deployment model allows a single user to have exclusive access to their own hardware and resources, providing greater control and flexibility. The cloud platform is implemented in a cloud-based secure environment that is protected by powerful firewalls and under the supervision of an organization's IT department.



Picture - 3[9]

c. *Hybrid Cloud* - Hybrid cloud computing combines proprietary software to bridge the public and private worlds, allowing organizations to host applications securely while benefiting from cost savings in the public cloud, and enabling the movement of

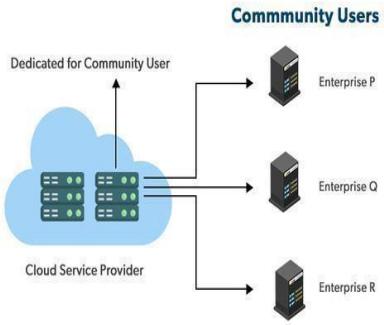


[8]*Cloud Deployment Models - GeeksforGeeks*, GeeksforGeeks, https://www.geeksforgeeks.org/cloud-deployment-models/ (last visited Aug. 14, 2024).
[9]*Cloud Deployment Models - GeeksforGeeks*, GeeksforGeeks, https://www.geeksforgeeks.org/cloud-deployment-models/ (last visited Aug. 14, 2024).

data and applications between different cloud deployment methods.

Picture - 4[10]

d. *Community Cloud* - A community cloud is a distributed system that integrates the services of different clouds to meet the specific needs of a group of organizations, typically managed by a third party or a combination of organizations within the community. The infrastructure of the community could be shared between the organization which has shared concerns or tasks.



Picture - 5[11]

5. *Cloud-based Services*

Cloud computing is the practice of using remote servers on the internet to store, manage, and process data, with cloud providers charging based on usage, and grids and clusters serving as the foundations for this technology.

Before the technology of cloud computing the user followed the traditional approach to accessing and managing the data, which is known as the On-premises Model which clearly says that for any business structure, the data centers should be on-site and should be maintained on their own. The user will be managing all the applications, data, Run-Time, Middleware, Operating Systems, Virtualization, Servers, Storage, and Networking on their own without depending on any other entity. This was a very expensive and time-consuming process. Due to the less flexibility in this approach, the new cloud computing service models have arrived in cyberspace.

a. *Types of Cloud Computing*

Most cloud computing services fall into the following categories:

i. Software as a Service (SaaS)

[10]*Cloud Deployment Models - GeeksforGeeks*, GeeksforGeeks, https://www.geeksforgeeks.org/cloud-deployment-models/ (last visited Aug. 14, 2024).
[11]*Cloud Deployment Models - GeeksforGeeks*, GeeksforGeeks, https://www.geeksforgeeks.org/cloud-deployment-models/ (last visited Aug. 14, 2024).

This is a method of accessing and using applications over the internet, eliminating the need for software installation and maintenance, and allowing users to run applications directly from a web browser. The SaaS applications are sometimes called Web-based software, on-demand software, or hosted software. E.g., Microsoft One Drive, Dropbox, WordPress, Office 365, and Amazon Kindle. SaaS is used to minimize the operational cost to the maximum extent.

ii. Platform as a Service (PaaS)

This is a cloud computing category that provides a platform and environment for developers to build applications and services over the Internet. PaaS frees users from the need to install in-house hardware and software, as the development and deployment of applications take place independently of the hardware. Users have control over the deployed applications and configuration settings for the application-hosting environment. The developer is responsible for the application, and the PaaS vendor provides the ability to deploy and run it. Using PaaS, the flexibility gets reduced, but the management of the environment is taken care of by the cloud vendors.

iii. Infrastructure as a Service (IaaS)

This is a service model that provides outsourced computer infrastructure, including networking equipment, devices, databases, and web servers, on a per-user basis, allowing users to access and utilize underlying operating systems, security, networking, and servers for developing applications and deploying development tools and databases. We can create a VM running Windows or Linux and install anything we want on it. Using IaaS, we don't need to care about the hardware or virtualization software, but other than that, we do have to manage everything else. Using IaaS, we get maximum flexibility, but still, we need to put more effort into maintenance.

III. Challenges

1. Challenges in Cloud Computing

Cloud computing has gained significant popularity in India, as it has globally, due to its scalability, cost-effectiveness, and accessibility. However, like in other countries, India faces several challenges related to cloud computing adoption. Unlike, conventional service providers, vendors of cloud computing solutions or cloud computing service providers do not cater to a single organization, but cater to hundreds and thousands of organizations and end users over a single virtual infrastructure located somewhere over the Internet. Hence, organizations need to undertake assurances from such vendors and service providers that their data hosted on virtual infrastructure is safe and secured.

Here are some of the key challenges that may be faced in a cloud computing environment and have also provided insights from an Indian law perspective.[12]

a. *Cyber Crimes*: Cybercrime has evolved alongside technology and impacts various sectors, including banking, e-commerce, and cloud services. A recent cyber-attack called 'Crypto jacking' involves infiltrating cloud servers to mine cryptocurrencies, often going undetected. Data breaches are another prevalent form of cybercrime, where unauthorized access or data copying occurs. India has faced significant cloud-related cyber-attacks in the past, like the Dropbox server breach in 2012, Yahoo's data breach in 2013[13], the 2016 Union Bank of India Heist, the WannaCry attack in 2017, and the data theft incident at Zomato in the same year. These incidents highlight the evolving landscape of cyber threats in the digital age.

b. *Data Breach*: Cloud providers often manage huge amounts of personal data from millions of users of cloud service, and the data from one user comes and mingles with the 4 data of other users. Also, there could be instances where a cloud service provider may be dealing with highly sensitive data for and on behalf of various organizations that may be competitors. Once an organization’s data is on the public cloud or the organization’s server, it should ensure all reasonable methods are used to protect such data. Thus, vendor contracts need to specify

[12]*Cloud Computing and Challenges faced in Existing Legal Structure*, SCC OnLine, 2.1 JCLJ (2021) 483.
[13]BBC, *Yahoo 2013 data breach hit all three billion accounts*, October 4, 2017, https://www.bbc.com/news/business-41493494. (last visited August 13, 2024).

control mechanisms so as to ensure the secrecy and protection of data[14]. Hence, the safeguarding and security of software and data is perhaps one of the foremost concerns in a shared third-party outsourcing arrangement[15].

There was a debate on cloud computing and privacy from a settlement in ***Author's Guild, Inc.* v. *Google Inc.*[16]** The stipulations of the agreement permitted Google to keep on offering copies of books on their cloud-based Google Books platform in return for a stipulated amount to the authors. Although, privacy was not the main concern in the settlement, many public interest organizations were alarmed that the agreement did not acknowledge the security of the privacy of its users. The settlement agreement did not address whether a user's reading preferences could be shared with news outlets or governmental units acting without a search warrant. Consumer Watchdog was concerned that the settlement gave Google a monopoly over the book search and book subscription markets and at the same time gave it unrestrained authority to share private information about users with outside entities[17].

c. *Privacy*: Cloud users should be cautious about data security and privacy, especially for sensitive information, as data breaches can occur due to system vulnerabilities. Privacy laws vary by server location, making jurisdiction awareness crucial. Cloud providers follow standards and laws but are not infallible. Data can be stored encrypted, but legal provisions may allow government access for non-law enforcement purposes.

d. *Data Protection*: Take the case of a simple Cloud-based email service, in which the data may be stored anywhere in the world. Depending on where the sender and recipient are, the data may circulate freely around the globe via the internet, using mirror servers for access and storage. Thus, it is not irrefutably clear which

[14] *Shaping Europe's Digital Future: Backbone Networks for Pan-European Cloud Federations*, EUROPEAN COMMISSION, Europa, October 21, 2022, https://digital-strategy.ec.europa.eu/en/activities/backbone-networks-cloud-federations. (last visited March 25, 2024).

[15] Santosh Bulusu & Kalyan Sudia, *A study on Cloud Computing Security Challenges*, 2012, Thesis no: MSE-2012:82, BLEKINGE INSTITUTE OF TECHNOLOGY, https://www.diva-portal.org/smash/get/diva2:830115/FULLTEXT01.pdf.

[16] Authors Guild v. Google, Inc., No. 13-4829 (2d Cir. 2015). (last visited March 20, 2024).

[17] Pritish Sahoo & Taruna Jaiswal, *Cloud Computing and its Legalities in India*, MANUPATRA INTELLECTUAL PROPERTY RIGHTS, July 2014, https://docs.manupatra.in/newsline/articles/Upload/7796F62A-E75D-45FD-8EC7-3AC01A4A5C7A.pdf. (last visited March 20, 2024).

data protection authorities at which location are responsible for ensuring the observance of the principles of data protection.

e. *Loss of Data*: Data loss is a significant concern for both cloud service users and providers. Despite not being physically stored locally, data is stored in a physical database, making it susceptible to loss from system failures, technical problems, or maintenance issues, often due to human errors in storage hardware. Responsibility for data loss falls under the shared responsibility model, with providers responsible for system infrastructure, but users accountable for their data's nature. Service providers do not compensate for data loss, placing the burden on the user, which can harm their reputation. Additionally, reliance on third-party vendors can lead to complications, potentially endangering user data due to contractual failures and conflicts with service providers.

f. *Non-Negotiable Contracts*: Cloud computing contracts, known as Service-Level Agreements (SLAs), adhere to legal conditions outlined in Section 10 of the Contract Act of 1872. These agreements are often non-negotiable and standardized, designed to serve a broad user base, following a 'click-wrap' approach. In this model, the cloud service provider sets fixed terms and conditions on electronic media, and users must accept them to access the service. While users are asked for consent, they usually accept the terms without changes due to limited alternatives, which can be seen as superficial consent. These agreements commonly include clauses about data sharing and user responsibility in data-related incidents. Users often overlook these terms, inadvertently risking their personal data and information security.

g. *Jurisdiction*: According to the traditional rules of private international law, the jurisdiction of a nation only extends to individuals who are within the country or to the transactions and events that occur within the natural borders of the nation, but time has changed.

In a cloud computing environment, an organization that is a resident of one country may store data on a cloud that is located in a different country and such

cloud may belong to a vendor who is located in a third country. Thus, there could be a situation whereby the laws of three jurisdictions are applicable.[18]

Subject to the laws/dispute resolution mechanism agreed under the definitive agreement, if there is any problem faced by the organization while accessing the data from the cloud or when there is any infringement action, the question that would then arise is, which is the appropriate jurisdiction for the purposes of ascertaining the cause of action for initiating a claim. Will it be the country where the server or data center is located where the infringing act took place or where the parties reside? In addition to this, the USA and most member states of the European Union have directives or laws on data privacy which may also encompass jurisdictional forums.

When it comes to the USA specifically, privacy laws vary from state to state within it. For example, a law in Massachusetts requires anyone who holds personal information belonging to a Massachusetts resident to implement a detailed written security program to protect the data. Companies subject to these regulations that want to implement cloud computing must determine whether the cloud provider maintains adequate security measures to protect its electronic data. Because a Massachusetts resident's data could be commingled with the data of many other users in the cloud, it would be difficult for cloud providers to know, which state regulations applied to such providers. Therefore, various factors would need to be considered while determining an appropriate jurisdiction along with the harmonization of domestic laws of each applicable country, to avoid conflict of laws.[19]

h. *Compliance*: Cloud-based services are susceptible to compliance failures due to their multi-jurisdictional nature, making it impossible to adhere to the laws of all relevant territories. Contradictory or open-to-interpretation laws in different countries further complicate matters.

[18] Enforcing laws in the realm of cloud computing, cybercrimes, and data breaches is a significant challenge for states. The complexity of cloud service infrastructure, spread across multiple global locations, scatters jurisdiction, creating conflicts among various legal standards. Local laws and state control are often insufficient due to the cross-border nature of cloud services, leading to multiple jurisdictional claims over cloud-stored data. Some states mandate local data storage, while India allows extra-territorial jurisdiction with specific contract clauses, complicating remedies for international disputes.

[19] *Cloud Computing and challenges faced in Existing Legal Structure*., supra note 12.

i. *Integration and Service Level Challenges*: The data centers of cloud service providers are located in various jurisdictions and all the information of individuals and organizations is spread across the world and needs to be integrated. If the integration is not made, it will be a hurdle for individuals and organizations to get full access to their files. It is so often that the infrastructure of a customer is not compatible with the applications provided by the cloud service provider, which as a result will have an impact on the working of cloud computing and the whole purpose of cloud computing gets defeated in the first place. From a single service provider, multiple customers can have access to cloud services. The level of service can vary from provider to provider, the organizations have to make sure that the services given to them by a cloud service provider are right on time and the response is quick, this is done because the data centers are located in different jurisdictions and it will be hard for any organization to commit to cloud computing when the services given to them will not be guaranteed[20].

Also, cloud computing adopts the availability of shared resources from various third parties. In such a scenario, service levels may differ from provider to provider and hence organizations have to ensure that service levels are not compromised and are consistently maintained. Conversely, if the data and applications are accessed from an organization's server, then it is easy to control the IT environment in which the data and applications are accessed[21]. But this is not true when the data resides over the cloud. Cloud providers may not be able to guarantee response time or service or quality levels because the data and applications may be on multiple servers hosted in various jurisdictions. Till there is a concrete solution on service or quality level guarantees, cloud computing may prevent organizations from migrating their critical and existing enterprise applications onto the cloud[22].

2. ***Few case studies***:

a. *The leak of CoWIN vaccination data***:**

[20] British Sahoo and Taruna Jaiswal., supra note 17.
[21] British Sahoo and Taruna Jaiswal., supra note 17.
[22] Nishith Desai, *Cloud Computing Risks/Challenges, Legal and Tax Issues*, NISHIT DESAI ASSOCIATES, Issues 1, 17, March 2023, https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Cloud_Computing.pdf. (last visited March 20, 2024).

There were a few allegations that there were data breaches of beneficiaries who received COVID-19 vaccination. As per reports, the current data breach is possible, if the mobile number of a person is entered; details such as the identification number of the document submitted for vaccination (Aadhaar, passport, PAN card, and so forth), gender, date of birth, and the center where the vaccine was administered, are provided as a reply in an instant by the messenger bot in question.

These details could be accessed even if the Aadhaar number was entered instead of the phone number. The passport numbers of those who had updated the CoWIN portal for travel abroad were also leaked[23].

The Union Health Ministry, however, said it requested the CERT-In to investigate this issue and submit a report. In addition, an internal exercise has been initiated to review the existing security measures of CoWIN.

The details, now available in the public domain through the leak, include those of Ram Sewak Sarma, chairman of CoWIN high power panel (the leak gives information on the ID papers submitted for vaccination), senior BJP leader Meenakshi Lekhi and Congress general secretary K.C. Venugopal (location at which they got vaccinated), the mode of registration for Kerala Health Minister Veena George[24].

The bot (a program that behaves like a normal chat partner with additional functions) on Telegram - is also giving details of individuals and several Opposition leaders' data including - Rajya Sabha member and Trinamool Congress leader Derek O'Brien, former Union Minister P. Chidambaram, Congress leaders Jairam Ramesh, Rajya Sabha Deputy Chairman Harivansh Narayan Singh, Rajya Sabha members Sushmita Dev, Abhishek Manu Singhvi, and Sanjay Raut among others[25].

While the bot has now been taken down, but the anxiety about the safety of personal data is still there. This is not the first time that such a leak has been reported. In June 2021, a hacker group named 'Dark Leak Market' claimed that it had a database of about 15 crore Indians who registered themselves on the CoWIN portal.

b. Dominos data breach

[23] *Id.*
[24] *Id.*
[25] *Id.*

Dominos Pizza is a well-known international brand with a significant presence in India, where it offers online ordering and delivery services through its website and mobile app. In 2021, the company faced a data breach incident that compromised sensitive customer data[26].

i. Data Security: The breach exposed customer data, including personal information, addresses, email addresses, and payment details. This raised significant concerns about data security and privacy.
ii. Jurisdictional Challenges: Dominos global operations use cloud services to manage and store customer data. The breach in India brought forth jurisdictional challenges related to data protection laws and regulations that apply in the country.
iii. Legal Compliance: In India, data protection laws, particularly the Personal Data Protection Bill (PDPB), were still in development in 2021. The breach put a spotlight on the need for companies like Dominos to ensure they would comply with new data protection legislation when it comes into effect.

Right after the issue Dominos immediately initiated an investigation into the data breach, working to assess the extent of the incident and its impact on customers. Further, the company increased its data protection measures and enhanced security protocols to prevent future breaches. It also engaged legal experts to understand the implications of India's evolving data protection laws and to ensure compliance once the PDPB is enacted. Finally, the immediate and appreciable action taken by Dominos was to communicate with affected customers, informing them of the breach and providing guidance on steps they could take to protect their personal information[27].

The Dominos data breach in India serves as a real-world example of jurisdictional challenges in the context of cloud computing. The breach raised concerns related to data security and the evolving legal landscape in India, particularly in the context of the PDPB. Companies operating in multiple jurisdictions, like Dominos, must navigate

[26]*Domino's India data breach: Name, location, mobile number, email of 18 crore orders up for sale on dark web* (May 25, 2021), https://www.firstpost.com/tech/news-analysis/dominos-india-data-breach-name-location-mobile-number-email-of-18-crore-orders-up-for-sale-on-dark-web-9650591.html#:~:text=To%20recall%2C%20it%20was%20only,a%20million%20credit%20card%20details. (last visited March 25, 2024).

[27]*Id*.

a complex web of data protection laws, and it is critical to stay updated on evolving regulations, maintain robust data protection measures, and have a clear response plan in place to address data breaches.

II. Future Aspects

The regulation of cloud computing in India is expected to evolve and adapt to the changing landscape of technology and data. The future aspects and the way forward for the regulation of cloud computing in India may include the following:

1. ***Data Protection Legislation:*** India is working on the implementation of comprehensive data protection legislation, the Digital Personal Data Protection Act, 2023. This Act sets stringent rules for data protection and privacy. The way forward involves implementing the Act, which will have a significant impact on how data is handled in the cloud. The Digital Personal Data Protection Act aims to regulate the collection, storage, processing, and transfer of personal data in India. It will define the rights of individuals, the obligations of data processors, and the role of a Data Protection Authority. The legislation provides clarity on how personal data should be handled within cloud computing services, ensuring the privacy and security of individuals data.
2. ***Data Localization:*** Data localization rules mandate that certain types of data be stored and processed within India. The future of data localization will involve defining the categories of data that must be localized and ensuring that cloud service providers have the necessary infrastructure to comply with these regulations. Clear guidelines on data classification and localization requirements will be essential. India has had a strong focus on data localization, requiring certain categories of sensitive data to be stored and processed within the country. The future of this regulation may involve clarifications and updates on which data should be localized and how it should be managed in the cloud.
3. ***Cloud Service Provider Certification:*** Certification of cloud service providers involves establishing standards for data security, compliance, and reliability. This may involve the creation of a certification body or authority that assesses and certifies cloud providers, ensuring they meet these standards. It can help businesses make more informed decisions about which providers to trust with their data. As the importance of cloud computing grows, there might be initiatives to standardize and certify cloud service providers to

ensure they meet specific security and privacy standards. This could enhance trust in cloud services.

4. ***Emergence of more competition:*** Given the four forms of cloud service, there is ample room for hundreds or even thousands of players in the market. As such, there will be many "large clouds" and a lot more "small clouds". Many of the small clouds will live on some of the large clouds, that is, many small cloud computing vendors will offer their services on the utility computing services provided by large cloud computing vendors.
5. ***Emergence of cloud integration services:*** Once the users start using services from multiple cloud service providers, the need will arise for migrating and integrating applications and data from different clouds. This will bring about a new form of cloud service, that is, cloud integration service. The integration technology will leverage such technologies as EAI (enterprise application integration), EII (enterprise information integration or federated database), and ESB (enterprise service bus).
6. ***Adoption of hybrid systems:*** Because one cannot reasonably expect cloud computing to guarantee 100% availability and security, many users will adopt hybrid systems of clouds and on-premises systems. The on-premises systems may include private clouds, that is, virtual data centers running within the firewall rising subscription fees The current low subscription fees are likely to go upwards significantly, as vendors harden their clouds (for higher performance, scalability, availability, and security), make their services richer, provide better support, and inevitably become profit-driven.
7. ***Security and Compliance Standards:*** Indian regulators are likely to establish clear security and compliance standards for cloud service providers and it may encompass encryption protocols, access controls, data breach response protocols, and compliance with industry-specific regulations (e.g., healthcare, financial services). Cloud providers will need to adhere to these standards to operate in India. These standards will ensure that providers adhere to best practices for data security and privacy.
8. ***Cross-Border Data Flow:*** The regulation may address cross-border data flows and the mechanism for the lawful transfer of data outside India. International data transfer agreements and frameworks, might involve standard contractual clauses and bilateral agreements with other countries.

9. ***Cybersecurity Regulations:*** In addition to data protection, regulations may focus on enhancing cybersecurity in cloud computing. This includes measures to prevent data breaches, ensure incident reporting, and impose penalties for security lapses. Regular security audits and assessments might be required to ensure compliance.
10. ***Cloud Service Agreements:*** Regulators may encourage transparency in cloud service agreements, ensuring that businesses understand the terms and conditions and their rights and responsibilities. This will help protect the interests of businesses and individuals who use cloud services. It may involve standardizing contract terms and ensuring that users are aware of their rights and responsibilities.
11. ***Adaptation to Technological Changes:*** As cloud computing technology evolves, regulations must adapt accordingly. The regulators will need to stay up to date with emerging technologies and their implications for data protection and security.
12. ***Enforcement and Penalties:*** Effective enforcement mechanisms will be essential to ensure that regulations are followed. Penalties for non-compliance may be introduced to discourage violations.
13. ***International Alignment:*** India will likely work on aligning its cloud computing regulations with international standards and practices, making it easier for Indian businesses to engage in global trade.
14. ***Large-scale collaborations:*** India has been at the forefront in setting examples for a digital revolution, be it through the rollout of Aadhar, UPI, or E-governance. And today, as its ushers towards 'Digital India', cloud maturity becomes imperative for both the government and enterprises to leapfrog another wave of digital transformation. However, large-scale adoption of the cloud and cloud-based services requires multi-stake collaboration that can address the common perceptions and barriers of the adoption process. The biggest challenge we are facing is the quality of education. There are many perennial gaps in the curriculum offered by Indian institutions and the skills required in the cloud job market.

The future of cloud computing regulation in India will involve a delicate balance between data protection, economic growth, and technological advancement. The government will need to work closely with industry players and other stakeholders to create a regulatory framework that fosters innovation and protects the rights and privacy of individuals and organizations using cloud

services. This framework should be flexible enough to adapt to the rapidly evolving cloud technology landscape while maintaining strong data protection and cybersecurity measures.

III. Conclusion and suggestions

1. Conclusion

In summation, our foray into the expansive domain of cloud computing unveils a technological landscape marked by innovation, connectivity, and multifaceted legal considerations. The historical trajectory, akin to the evolution of legal doctrines, has seen the conceptualization of utility computing and the transformative impact of Virtualization, mirroring the dynamic nature of legal precedents and jurisprudential developments.

The architectural foundations of cloud computing, resembling the intricate framework of legal systems, exhibit a nuanced interplay of public, private, and hybrid deployment models. This structural complexity is further reflected in the diverse array of services hosted within these virtual realms, akin to the legal principles governing distinct facets of legal practice.

Yet, amidst the technological marvels, the legal scholar lens discerns the intricate challenges posed by privacy protection, a legal terrain where notions of informational autonomy and data sovereignty intersect. The looming specter of cybercrimes, reminiscent of legal transgressions, raises questions regarding the efficacy of regulatory frameworks and the imperative for robust cybersecurity measures.

Many organizations may not be forthcoming to put their data and applications over the cloud instantaneously, it is because of the challenges that are associated with its use that primarily includes data breach this is because Data protection and security are paramount in cloud computing. While India has taken steps to enhance data protection through laws like the Digital Personal Data Protection Act 2023, questions regarding the scope and enforcement of these measures still remain.

Cross-border data flows and international agreements also play a significant role in cloud computing. India's participation in such agreements affects the movement of data and the regulatory environment.

2. Suggestions

Addressing these issues in cloud computing requires a combination of technical, legal, and organizational measures. Here are some suggestions:

a. *Privacy*:
    i. Encryption: Implement strong encryption for data both in transit and at rest to protect sensitive information.
    ii. Data Minimization: Only store and process the data necessary for the service, reducing the risk associated with handling excessive information.

b. Jurisdiction:
    i. Contractual Agreements: Clearly define jurisdiction in service level agreements (SLAs) to avoid legal ambiguities.
    ii. Hybrid Cloud Solutions: Consider hybrid cloud models that allow sensitive data to be stored on-premises or in a specific jurisdiction.

c. Non-negotiable Contracts:
    i. Negotiate Terms: If possible, negotiate specific terms with the cloud service provider to tailor the contract to your organization's needs.
    ii. Explore Alternatives: Consider alternative providers that may offer more flexibility in contract negotiations.

d. Compliance:
    i. Audit and Certification: Choose cloud providers that adhere to industry-specific compliance standards and obtain relevant certifications.
    ii. Regular Audits: Conduct regular audits to ensure ongoing compliance with relevant regulations and standards.

e. Data Protection:
    i. Access Controls: Implement robust access controls to restrict data access only to authorized personnel.
    ii. Regular Backups: Regularly back up critical data and ensure a solid disaster recovery plan is in place.

f. Cyber Crimes:
    i. Security Measures: Invest in advanced cybersecurity measures, including firewalls, intrusion detection systems, and regular security audits.

ii. Employee Training: Educate employees on cybersecurity best practices to reduce the risk of social engineering attacks.

g. Loss of Data:

i. Data Backups: Regularly back up data and ensure reliable recovery mechanisms are in place.

ii. Redundancy: Utilize redundant systems and geographically distributed data centers to minimize the risk of data loss.

It is important to tailor these suggestions to the specific context and requirements of your organization. Regularly reviewing and updating security measures, staying informed about legal and regulatory changes, and fostering a security-conscious culture within the organization are ongoing processes crucial for maintaining a secure cloud environment.

CLOUD CONUNDRUM: NAVIGATING LEGAL SKIES IN INDIA AND BEYOND

- *Velanati Jyothirmai & Koppala Nikhil*[1]

Abstract

In the ever-evolving digital landscape, the rise of cloud computing has transformed business operations, introducing unprecedented flexibility and scalability. As organizations embrace cloud solutions, legal considerations and challenges in this realm become central to discussions. While the advantages of cloud adoption are evident, legal complexities arise, focusing on data protection, contractual issues, and service-level agreements. Regulatory compliance adds another layer of challenge, with cloud service providers navigating diverse frameworks. When we look at the legal landscapes in the US, China, and the EU reveals substantial variations. Hence, to thrive, India must adopt global best practices, necessitating a comparative study of international laws. Implementing select practices is crucial for adapting to the evolving interplay between technology and the law, ensuring India's seamless integration into the global cloud computing landscape.

Keywords: *Cloud Computing, Legal Challenges, Data Protection, Regulatory Compliance, Global Best Practices*

[1] 5th Year, BA.LLB., DamodaramSanjivayya National Law University. Gmail: jyothirmaivelanati@dsnlu.ac.in&koppalanikhil@dsnlu.ac.in

I. Introduction

Cloud computing has emerged as a transformative force in the field of information technology, reshaping the way businesses and individuals' access, store, and process data. At its core, cloud computing involves delivering computing services, including storage, processing power, and applications, over the Internet. This paradigm shift has significantly impacted various sectors, offering unparalleled flexibility, scalability, and cost-effectiveness.

One of the key advantages of cloud computing is the ability to access resources on demand. Instead of relying on local servers and infrastructure, users can tap into a vast network of remote servers hosted by third-party providers. This flexibility enables businesses to scale their operations efficiently, adapting to changing demands without the need for significant upfront investments in hardware. The cloud computing model comprises three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides virtualized computing resources over the internet, PaaS offers a platform for developers to build and deploy applications, and SaaS delivers software applications directly to end-users.

Security and data privacy are critical considerations in cloud computing. Reputable cloud service providers implement robust security measures, including encryption and authentication protocols, to safeguard data. However, users must also be vigilant about configuring and managing their cloud resources securely, as misconfigurations can pose risks.

The benefits of cloud computing extend beyond businesses, influencing individuals through services like cloud-based storage, email, and collaboration tools. The accessibility and convenience of cloud services have become integral to modern work and lifestyle.

As the landscape of technology continues to evolve, cloud computing is likely to play an even more pivotal role. Innovations such as edge computing and hybrid cloud solutions are further expanding the possibilities, providing tailored solutions to meet the diverse needs of users. With ongoing advancements and an increasing reliance on digital infrastructure, the impact of cloud computing on how we live and work is set to deepen in the years to come.

II. Legal Framework

Cloud computing in India is subject to various existing laws and regulations that govern data privacy, cybersecurity, and technology transactions. These laws may have an impact on cloud computing services and their usage. Here are some key legislations and regulations in India that are relevant to cloud computing:

1. Domestic Laws

a. Information Technology Act, 2000 (IT Act)

Several sections of the IT Act are relevant to cloud computing, particularly concerning data protection, cybersecurity, and liability. Section 43A requires companies handling sensitive personal data to implement reasonable security practices. Failure to do so and resulting data breaches may lead to liability for compensation to affected parties, which is particularly pertinent for cloud service providers storing sensitive client data. Sections 66, 66B, 66C, 66D, and 66E address computer-related offenses, identity theft, punishment for identity theft, cheating by personation, and violations of privacy, respectively, all of which can be applicable in cases related to cloud services.

Section 72 focuses on the breach of confidentiality and privacy, making it an offense to breach sensitive personal data confidentiality, a concern for cloud service providers entrusted with client data. Section 72A pertains to the punishment for unauthorized disclosure of personal information, and Section 79 outlines intermediaries' liability, imposing the responsibility to follow due diligence, especially relevant to cloud service providers in removing or blocking access to unlawful content.

i. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, (SPDI Rules)

These rules govern the handling of sensitive personal data in India. These rules have implications for organizations using cloud services for sensitive data. They define SPDI, require data protection measures, mandate due diligence for data transferred to the cloud, emphasize consent and notice, and address data retention.

Additionally, they cover concepts like SPDI disclosure and data breach notification.

b. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act of 2023 represents a significant shift in data protection in India. It defines key terms and responsibilities for data handling, emphasizing the need for informed consent. Notably, it prioritizes children's data protection, requiring parental consent and prohibiting tracking or targeted advertising for minors. Major data processors face increased obligations, promoting responsible data management. The Act establishes a Data Protection Board to enforce compliance and address grievances, while providing Data Principals with rights to access and correct their data. It also addresses international data flows, non-compliance penalties, and an appeals process, prioritizing transparency, accountability, and individual rights for a safer digital ecosystem.

c. RBI Guidelines

Cloud computing is a pay-per-use model that grants access to various computing resources, and categorizes them into service models (SaaS, PaaS, IaaS), and deployment models (private, community, public, hybrid). The advantages of cloud computing include cost efficiency, accessibility, agility, scalability, and high availability. However, there are privacy concerns, as service providers may have access to stored data, and regulatory compliance may necessitate more expensive private cloud deployment.[2]

The Reserve Bank of India (RBI) underscores the importance of robust guidelines for financial institutions embracing cloud computing. As part of these guidelines, diligent vendor due diligence is mandated to ensure the selection of trustworthy cloud service providers. Emphasis is placed on establishing stringent data access and audit mechanisms, guaranteeing secure and accountable handling of sensitive financial information.[3]

[2] Notification - Master Direction on Outsourcing of Information Technology Services, issued by RBI on April 10, 2023, https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=12486, last accessed on 10th October, 2023.

[3] Various parties are involved in cloud deployment:

- Cloud consumer: Banks or consumers availing cloud services.

Furthermore, compliance and reporting frameworks are integral components, necessitating financial institutions to adhere to regulatory standards and promptly report any deviations. In line with proactive security measures, periodic security assessments are mandated, ensuring continuous evaluation and enhancement of cloud infrastructure resilience. These guidelines collectively aim to fortify the security and integrity of financial systems in the dynamic landscape of cloud computing.

d. *GST (Goods and Services Tax) Regulations*

i. Pre-GST Regime

In ***PSI Data Systems Ltd.* v. *CCE***[4], the main dispute of the case centered on excise duty assessment for computers with software. The court by referring to the example that when cassette and recorder are sold together the recorder is not taxed along with the value of the cassette, has ruled that software sold with computers should not be considered part of the computers, as software is a for excise duty. This decision was challenged in ***Tata Consultancy Services* v. *State of Andhra Pradesh***[5], leading to a reference for further consideration. In ***Commissioner of Central Excise v. Acer India***[6], the issue resurfaced, focusing on central excise law. A three-judge panel in ***CCE* v. *Acer India (2004)*** affirmed that excise duty should not be imposed on combined computer and software values. However, in ***Tata Consultancy Services* v. *The State of AP.***[7] Case, a Constitution Bench established that marketable and useful software qualifies as 'goods,' regardless of its intellectual property status, as they are sold through CD ROMs, discs, floppies, etc. This precedent emphasized equal treatment for tangible and intangible property in Indian law.

A. Relevance of these cases with Cloud Computing

- Cloud provider: System integrators offering solutions, comprising data center and hardware providers, infrastructure software providers, virtualization software providers, application providers, and network providers.
- Cloud carrier: Providers of network infrastructure connecting bank branches to data centers.
- Cloud auditor: Reputed audit firms conducting independent security, data privacy, and performance audits.

Cloud broker: Parties offering value-added services on top of cloud providers' services, such as aggregation or arbitration.

[4] PSI Data Systems Ltd. v. CCE, (1997) 2 SCC 78.

[5] Tata Consultancy Services v. State of Andhra Pradesh, (2001) 4 SCC 629 (First TCS Case).

[6] Commissioner of Central Excise v. Acer India, (2004) 10 SCC 111.

[7] Commissioner of Central. Excise v. Acer India Ltd., (2004) 8 S.C.C. 173.

The court determined the Second TCS Case does not apply to Cloud computing due to its reliance on physical media. The case clarifies that without a medium, no right transfer occurs, making State Legislatures unable to levy sales tax on Cloud computing transactions. Additionally, excise duty does not apply as Cloud computing does not involve hardware sales. It is deemed a service, and no software is "manufactured" within India's territory.[8]

ii. Post-GST Regime

***Amazon Web Services, Inc.* v. *CIT*[9]**

The Delhi Bench of the Income Tax Appellate Tribunal (ITAT) ruled that Amazon Web Services (AWS) cloud computing services are not subject to taxation in India as royalty or fees for technical services (FTS or FIS). The ITAT held that AWS offers standardized services that don't provide technical knowledge for future independent use, failing the "make available" test. AWS, a US-based company, was reassessed for the assessment years 2014-15 and 2016-17, with the department arguing for taxation. The ITAT emphasized that AWS's services were standard and automated, available online to all, and did not grant rights to use intellectual property, aligning with the India-USA Double Taxation Avoidance Agreement.

Section 2(17) of the Integrated Goods and Services (IGST) Act, 2017, defined OIDAR services as automated services delivered via the Internet with minimal human intervention. The Finance Act of 2023 broadened the scope, removing the "minimal human intervention" requirement. Online Information Database Access and Retrieval (OIDAR) services are now subject to an 18% GST rate in India. Starting from October 1, 2023, foreign OIDAR service providers are no longer exempt from GST, leading to a

[8] The absence of physical media in Cloud computing transactions distinguishes them from traditional software sales. Furthermore, the BSNL v. Union of India, (2006) 3 SCC 1highlights that the deeming fiction created under Article 366(29A) (d) of the Indian Constitution should not be used to levy sales tax on Cloud computing transactions, as such a move would require an artificial declaration of these transactions as sales. The scope of Article 366(29A) (d) does not allow for such flexibility. Hence, it is not appropriate to impose sales tax on cloud computing transactions, and they should be categorized as services rather than sales of goods.

[9] Amazon Web Services, Inc. v. CIT, 2023 SCC OnLine ITAT 584.

mandatory 18% GST for services to individuals and the government, irrespective of their intended use.

e. *Intellectual Property Laws*

Cloud computing's growing popularity offers efficient data storage but poses IP risks due to limited control and data location uncertainty. The global nature of the cloud complicates matters, as IP laws vary. India lacks specific cloud computing laws, and existing ones focus on data security. To manage IP risks, due diligence in selecting secure cloud service providers and robust IP protection clauses in contracts are crucial. Encryption and automated data handling enhance security. Despite risks, cloud adoption is rising in India, necessitating adaptable IP laws to safeguard intellectual assets. Preparing for worst-case scenarios is vital for IP protection in the cloud.

III. Laws of Various Nations

a. Regulation of Cloud Computing in the European Union

Cloud computing is a widespread technology bringing important benefits to millions of consumers and enterprises across the world. According to a recent report, cloud computing is the most widely adopted technology across industries.[10] Cloud computing is also being used in public administration and has important applications in the daily lives of consumers, ranging from streaming platforms to email services. In addition, cloud computing plays a crucial role in facilitating the uptake of key emerging technologies and applications such as artificial intelligence, blockchain, the Internet of Things, and high-performance computing.[11]

Considering the versatility and efficiency of cloud computing, it is not surprising that the value of the global cloud computing market is on track to exceed 1 trillion dollars by

[10] Gabriella Cattaneo, Filippo Vanara, et al., *Advanced Technologies for Industry – AT Watch: Technology Focus on Cloud Computing*, ATI WATCH REPORT SERIES, EUROPEAN COMMISSION, Europa, December 2020, at 14-20.

[11] *Shaping Europe's Digital Future: Backbone Networks for Pan-European Cloud Federations*, EUROPEAN COMMISSION, Europa, October 21, 2022, https://digital-strategy.ec.europa.eu/en/activities/backbone-networks-cloud-federations, last accessed on 12th October 2023.

2030. The current growth will likely be accelerated by the increasing popularity of new applications of cloud computing technology, such as cloud gaming.[12]

Despite its potential, many businesses do not use cloud computing. This highlights the need for a more widespread adoption of the technology. The EU is the first jurisdiction that has adopted sector-specific rules for cloud computing. The EU intends to regulate Cloud Computing with three enactments Digital Markets Act (DMA), the Digital Services Act, 2022 (DSA), and the proposal for the Data Act, 2023 (DA). It follows that these three Acts will serve as prominent examples for other jurisdictions that are adopting their own regulation.

i. Cloud Computing Services under the DSA

A. Objectives of the DSA:

The Digital Services Act (DSA) is designed to regulate intermediary services, ensuring a safe, predictable, and trusted online environment while protecting fundamental rights. It establishes rules for intermediary services, liability exemptions, and due diligence obligations based on the size and type of intermediary service.[13]

B. Implications of Including Cloud Services in the DSA:

The DSA, in its current form, categorizes cloud services as hosting services or online platforms.[14] However, this categorization has raised concerns regarding its applicability to cloud computing.

i. Broad Scope of Hosting Services: The definition of hosting services in the DSA is broad, encompassing services provided to enterprises that might not be equipped to handle obligations related to content removal. This ambiguity affects how cloud services, especially those targeting enterprises, would comply with DSA obligations.

ii. Definition of Online Platforms: Cloud services could also qualify as online platforms based on the dissemination of information to the public. However, the DSA does not provide a clear definition of what constitutes

[12] *Cloud Gaming Market Size, Share & Trends Analysis Report by Type (File Streaming, Video Streaming), By Device, By Gamer Type, By Region, and Segment Forecasts, 2022–2030*, GRAND VIEW RESEARCH, 2023, https://www.grandviewresearch.com/industry-analysis/cloud-gaming-market, last accessed on 12th October, 2023.

[13] DSA (n 7) Article 1(1).

[14] *Id.* at Recital (27a).

the "public", leading to potential over interpretation of the term. For example, services like OneDrive could inadvertently fall under online platforms despite their primary function as cloud storage.

To ensure that cloud services are appropriately regulated under the DSA, it is crucial to define terms like "public" within the context of cloud computing and avoid inadvertently subjecting cloud providers to obligations meant for other types of digital services.

ii. Cloud Computing Services under DMA

A. Objectives of the DMA:

The Digital Markets Act (DMA) has been introduced in response to the growing significance of online platforms in the European economy. The DMA primarily aims to address concerns related to the market power of certain online platforms, referred to as "gatekeepers". These gatekeepers are seen as central intermediaries connecting businesses with consumers, and the DMA seeks to address issues related to reduced competition, unfair practices, and the control exerted by these gatekeepers over the digital ecosystem.

B. Implications of Treating Cloud Services as Core Platform Services:

According to Article 3 of the DMA, an undertaking shall be designated as a 'gatekeeper' if it meets three overarching qualitative requirements, namely, it has a significant impact on the internal market; it operates a core platform service (CPS) that serves as an important gateway for business users to reach end-users; and it enjoys an entrenched and durable position in its operations. An undertaking is presumed to satisfy these qualitative conditions if it meets the quantitative thresholds laid down in Article 3(2).[15] The DMA's scope (including cloud computing services) has raised concerns on various fronts.

[15] Article 2(13), referring to Article 4(19) of Directive (EU) 2016/1148 of the European Parliament and of the Council.

i. *Contestability of the Cloud Computing Market:* One of the key objectives of the DMA is to improve contestability in digital markets. However, the cloud computing industry is marked by robust competition, with numerous providers vying for market share. This begs the question of why cloud services should be subject to the DMA, given that it's intended to safeguard competition in markets dominated by single platforms or oligopolies.

ii. *Lack of Multi-Sidedness in Cloud Services:* The DMA primarily targets digital platforms that serve as intermediaries connecting business users with end users. Cloud computing services, on the other hand, do not typically function as intermediaries between these two user groups. Instead, they provide tools and infrastructure to businesses for various operations like website hosting, data analytics, or network storage. Thus, cloud services don't exhibit the multi-sided nature that the DMA intends to regulate.

iii. *Difficulties in Identifying Users:* Designating cloud computing services as core platform services becomes problematic when attempting to identify and count the business and end users of these services. The DMA's quantitative thresholds for gatekeeper designation become ambiguous when applied to cloud services, given the complexity of interactions and users within cloud computing ecosystems.

C. Obligations for Gatekeepers under the DMA:

The DMA outlines various obligations for gatekeepers, but many of these obligations are specific to certain services like search engines or app stores. The obligations relevant to cloud computing services appear to be limited. For instance, the DMA restricts gatekeepers from requiring business or end users to subscribe to core platform services, but the relevance of such obligations to cloud services remains questionable.

As regards Article 5, the most relevant obligations are the requirement to obtain user consent to engage in data combination,[16] and the prohibition to require

[16] DMA (n 6) Article 5(2).

business users or end users to subscribe to any core platform services offered by a gatekeeper as a precondition for using its cloud services.[17]

D. Looking Forward: The European Commission has not yet designated any cloud computing providers as gatekeepers under the DMA. However, this does not rule out the possibility of future designations. If cloud providers are designated as gatekeepers, they may have opportunities to challenge this designation.

i. Rebutting Designation: Under the DMA, an undertaking meeting quantitative thresholds may challenge its designation as a gatekeeper. Cloud providers could argue that they do not function as "important gateways" for business users to reach end users, given their distinct role as service providers rather than intermediaries. They may use both quantitative and qualitative evidence to support their case, raising questions about the proportionality, non-discrimination, and due process of such designations.

ii. Challenging the DMA Itself: Cloud providers designated as gatekeepers may also challenge the DMA on the grounds that it is disproportionate and ill-suited to regulating services like cloud computing. This could be a legal avenue to question the appropriateness of the DMA's inclusion of cloud services within the category of core platform services.

In summary, the DMA's treatment of cloud computing services raises important questions about the regulation of digital markets and the need for careful consideration of the unique characteristics of cloud services when crafting digital regulations.

iii. Cloud Computing Services under the Proposed Data Act (DA)

A. Objectives of the Data Act:

[17] *Id.* at Article 5(8).

The Data Act (DA) aims to create fairness in the digital environment, stimulate a competitive data market, facilitate data-driven innovation, and make data more accessible. It introduces rights and obligations related to data access, switching between services, data transfer, and interoperability.[18]

B. Implications of Including Cloud Services in the Data Act:

The DA proposal has implications for cloud computing services due to its broad scope and obligations. However, the proposal raises concerns in its current form.

i. Lack of Clarity with respect to Scope: The DA's extensive scope, which includes personal and non-personal data[19], and its broad definitions of "data holders" create uncertainty about how user rights will be applied to cloud services. The distinction between cloud service providers and users or other entities that could be considered "data holders" is not clearly defined.

ii. Compliance Challenges Arising from Substantive Obligations: The DA proposes obligations to facilitate switching between data processing services of the same service type. However, the concept of "functional equivalence" in the context of cloud computing is unclear and ensuring full "functional equivalence" is challenging given the unique features of different cloud services. Additionally, compiling a list of all known "service types" for functional equivalence is impractical, as cloud services may have unique features or functionalities.

b. Regulation of Cloud Computing in China

Cloud computing has transformed the way businesses and individuals' access and store data, offering unparalleled convenience and efficiency. China, as one of the world's largest economies and a growing tech powerhouse, has embraced cloud computing as a key driver of innovation and economic growth. However, the rapid expansion of this

[18]Brussels, *Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy*, EUROPEAN COMMISSION, February 23, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113, last accessed on 13th October, 2023.

[19] DA proposal, Article 2(1).

technology has prompted Chinese authorities to establish a comprehensive legal framework to regulate cloud computing. This section deals with the key aspects of cloud computing law in China, exploring its regulatory environment, data protection, and the challenges and opportunities it presents.

i. Data Localization Requirements:

China's approach to data localization requirements is a fundamental aspect of its cloud computing regulation. These regulations dictate where data collected and processed in China must be stored and managed. There are two primary components within this subheading: Cross-border Data Transfer Rules and Data Storage and Processing Mandates.

Cross-border Data Transfer Rules: China has imposed strict controls on the transfer of data outside its borders. When data collected within China needs to be sent to servers or data centres located abroad, it often requires prior approval from regulatory authorities. This approval process involves rigorous assessments to ensure that data exports comply with data security and privacy standards. The purpose of these rules is to protect the security of data and reduce the risk of unauthorized access by foreign entities.

Data Storage and Processing Mandates: These mandates require certain types of data to be stored and processed within China's territorial boundaries. While the specifics can vary depending on the nature of the data, industries, and regulations, the general idea is to enhance data security by ensuring that data remains under Chinese jurisdiction. For instance, critical infrastructure data, sensitive personal data, and certain business data are often subject to these localization requirements.

In practice, this means that multinational companies and cloud service providers operating in China must establish data centers or partner with local data hosting services to comply with these requirements. The Chinese government's rationale for this approach is to maintain control and oversight over data generated within

its jurisdiction, thereby safeguarding national security and preventing potential data breaches.

Compliance with these data localization requirements is essential for businesses operating in China, as failure to do so can result in regulatory penalties, data access restrictions, and potential damage to a company's reputation. It also requires careful consideration when planning cross-border data operations, data centre investments, and cloud infrastructure deployments in China.

ii. Cyber security and Privacy Laws:

China has implemented a comprehensive framework of cybersecurity and privacy laws to govern the use of cloud computing services within its borders. To understand the framework of regulation of cloud computing in China we must analyse two critical aspects: Cybersecurity Law and Compliance and the Personal Information Protection Law (PIPL).

Cybersecurity Law and Compliance: China's Cybersecurity Law, enacted in 2017, is a foundational piece of legislation that places obligations on network operators, including cloud service providers, to ensure the security and integrity of their networks and data. Compliance with this law involves implementing security measures, reporting cybersecurity incidents promptly, and cooperating with government authorities to maintain national cybersecurity. The law also requires data localization and imposes certain restrictions on cross-border data transfers, particularly for personal and important data.

Personal Information Protection Law (PIPL): The PIPL, which came into effect on November 1, 2021, is China's comprehensive data privacy law. It regulates the collection, use, and protection of personal information and places stringent requirements on companies handling such data through cloud services. This includes obtaining informed consent from individuals, setting up data breach response mechanisms, and adhering to specific rules for cross-border data transfers. Companies must also appoint data protection officers to ensure compliance with PIPL's requirements.

These laws reflect China's commitment to enhancing data security, protecting individual privacy, and bolstering the country's cyber security defenses. They require cloud service providers to implement strict cybersecurity measures and data protection protocols. Failure to comply with these laws can result in penalties, legal actions, and business disruptions.

It's crucial for businesses operating within China to have robust data protection and cybersecurity strategies in place, as they must navigate complex regulations, ensure data security, and uphold privacy rights while delivering cloud services to a vast and growing market. Companies should be prepared to adapt to evolving cybersecurity and privacy regulations as the Chinese government refines its approach to these issues.

iii. Cloud Service Provider Licensing:

In China, the operation of cloud computing services is subject to strict licensing and regulatory requirements. To understand the framework of regulation of cloud computing in China we must address the necessity of obtaining licenses for cloud service providers and the ongoing compliance and oversight measures to ensure adherence to these regulations.

Licensing and Certification Requirements: China mandates that cloud service providers must obtain specific licenses to operate within its borders. These licenses are typically issued by government authorities and serve as proof that the provider complies with the regulatory standards for data security, service quality, and infrastructure reliability. These standards can cover a wide range of areas, from cybersecurity to data localization and operational integrity.

Compliance with these licensing requirements is essential for cloud providers, as operating without the required licenses can lead to legal consequences, business disruption, and damage to an organization's reputation. Providers must navigate a complex process to meet the necessary criteria and standards set by Chinese authorities.

Compliance and Oversight: After receiving the required licenses, cloud service providers are subject to ongoing compliance monitoring and oversight by regulatory bodies. This ensures that they maintain the standards outlined in their licenses and adhere to evolving regulations.

Regulatory oversight can involve regular audits, inspections, and reporting requirements. Non-compliance can lead to penalties, suspensions, or even the revocation of licenses, which can significantly impact a provider's ability to operate in the Chinese market.

These regulatory processes are in place to safeguard data security, protect consumers, and maintain the integrity of cloud services in China. They are designed to ensure that cloud providers meet stringent quality and security standards, which are vital in a country with a rapidly growing digital economy and increasing concerns about data protection and cybersecurity. Consequently, cloud service providers must prioritize compliance and navigate these intricate regulatory procedures to establish and maintain their presence in the Chinese market.

c. Regulation of Cloud Computing in the United States of America

i. Data Privacy and Security Regulations, including the CLOUD Act

In the United States, data privacy and security regulations are fundamental to the regulation of cloud computing, and they include the significant impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which was enacted in 2018.

The CLOUD Act of 2018 introduced significant changes to data privacy regulations in the United States. This law grants law enforcement agencies the authority to access data stored in the cloud, regardless of whether it is located within the United States or overseas. It also facilitates international agreements for cross-border data access, simplifying the process for law enforcement to

access data stored abroad.[20] The CLOUD Act has far-reaching implications for cloud service providers, as it may require them to comply with data access requests from U.S. law enforcement, even if the data is stored outside of the country. This aspect of the CLOUD Act raises important questions about the balance between law enforcement needs and individual privacy rights.

In the United States, compliance with data privacy and security regulations, including the CLOUD Act, is essential not only for legal reasons, but also to maintain customer trust and protect sensitive information. Cloud service providers must implement robust security measures, and data protection protocols, and be prepared to navigate the complex landscape of data access requests and cross-border data transfers brought about by the CLOUD Act.

The CLOUD Act asserts that U.S. data and communication companies must provide stored data for a customer or subscriber on any server they own and operate when requested by warrant, but provides mechanisms for the companies or the courts to reject or challenge these if they believe the request violates the privacy rights of the foreign country the data is stored in.[21]

It also provides an alternative and expedited route to MLATs through "executive agreements"; the executive branch is given the ability to enter into bilateral agreements with foreign countries to provide requested data related to its citizens in a streamlined manner, as long as the Attorney General, with the concurrence of the Secretary of State, agree that the foreign country has sufficient protections in place to restrict access to data related to United States citizens. The first such agreement was with the United Kingdom.

Cloud service providers and organizations utilizing cloud services are subject to cybersecurity regulations and data breach notification requirements. The Federal Trade Commission (FTC) plays a role in enforcing cybersecurity standards, ensuring that companies implement adequate security measures to protect data from breaches. Additionally, many states have their own data breach notification

[20] Halefom H Abraha, *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis, International Data Privacy Law*, OXFORD ACADEMIC, Volume 9, Issue 3, August 2019, Pages 207–215.
[21] *Id.* at 11

laws that require prompt reporting of data breaches to affected individuals and regulatory agencies.

ii. Government Surveillance and Data Access

It is necessary to understand the legal and regulatory framework surrounding government surveillance and data access in the United States, which significantly impacts cloud computing services.

The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) was enacted in the aftermath of the September 11, 2001 terrorist attacks. It grants the U.S. government broad surveillance powers for the purpose of national security and counterterrorism. Under this act, law enforcement agencies can obtain access to electronic records, including those held by cloud service providers, with appropriate legal authorization. The USA PATRIOT Act has raised concerns about privacy and data security, particularly for cloud service users concerned about government access to their data.

FISA Amendments Act and Foreign Intelligence Surveillance Court (FISC): The Foreign Intelligence Surveillance Act (FISA) Amendments Act and the Foreign Intelligence Surveillance Court (FISC) provide a legal framework for the collection of intelligence information, including electronic data. These laws allow intelligence agencies to seek court orders to access data, even if it is held by cloud service providers. The proceedings typically happen in secret, leading to discussions about the balance between national security and individual privacy.

The landscape of government surveillance and data access in the United States raises important questions about privacy and individual rights. For cloud service providers, it means adhering to legal requirements while respecting user expectations regarding data privacy and security. It’s crucial for organizations and cloud providers to understand the legal framework surrounding government surveillance and data access, as it can impact their data management strategies, particularly when dealing with sensitive or confidential information. Moreover, it

emphasizes the need for transparency and clear data access policies within cloud service agreements.

iii. International Data Transfers and Cross-Border Regulations

The European Union (EU) and the United States have had ongoing discussions and agreements related to data protection. One key agreement was the EU-U.S. Privacy Shield, which aimed to facilitate the transfer of personal data from the EU to the United States. However, it was invalidated by the European Court of Justice in 2020.[22] In its place, cloud service providers and organizations utilizing cloud services must consider compliance with the General Data Protection Regulation (GDPR), a comprehensive data privacy law that applies to the processing of personal data of individuals in the EU. GDPR requires stringent protections for personal data and sets specific rules for international data transfers. Compliance with these regulations is critical for cloud service providers to continue serving customers in the EU.

The United States has export control regulations that can impact cloud computing services, particularly when it comes to the export of encryption technologies and certain data processing activities. Understanding these regulations is important, as they can impact the types of cloud services that can be offered in specific international markets. Additionally, data sovereignty concerns arise as some countries require data to be stored within their borders. This raises challenges for cloud providers, especially when they operate globally and need to navigate differing data storage requirements.

Navigating international data transfer regulations and cross-border data management is a complex task for cloud service providers and organizations. These regulations underscore the importance of robust data protection measures, encryption, and clear data transfer policies. It's crucial to stay informed about changes in international data protection laws, as they can have far-reaching consequences for cloud computing services and the cross-border flow of data.

[22] Jaskaran Singh Saini, Dinesh Kumar Saini, et. al., *Cloud Computing: Legal Issues and Provision*, Security and Communication Networks, ACM DIGITAL LIBRARY, Volume 2022, 2022, https://doi.org/10.1155/2022/2288961, last accessed on 16th October, 2023.

d. Case Laws

***a. Neetu Singh* v. *Telegram FZ LLC*[23]**

FACTS

Neetu Singh and K.D. Campus Pvt. Ltd. has filed a lawsuit against Telegram FZ LLC and unknown individuals (John Doe) for copyright infringement, seeking an injunction, damages, and other remedies. The Plaintiffs claim that their educational content, including books and lectures, is being disseminated without authorization through various Telegram channels. Despite reporting the abuse to Telegram, some infringing channels remain, leading the Plaintiffs to seek legal action to protect their copyrighted works. The court has issued orders and is considering the Plaintiffs' application to discover the identities of the channel operators.

ISSUE

Whether Telegram can be compelled to disclose the identities of individuals, who are behind the infringing channels that disseminate the said copyrighted works without authorization.

PLAINTIFFS ARGUMENTS

Plaintiffs argue that Telegram's Privacy Policy obligates them to take down channels that violate the law and disclose information about those operating such channels. New channels are continually created to disseminate infringing materials, and revealing the identities of these individuals is necessary for the Plaintiffs to take legal action against them. It is also argued that Indian courts have jurisdiction over mobile platforms operating in India and should be able to issue directions regarding such platforms. She asserts that Singaporean law should not apply when a court order is issued.

DEFENDANT'S ARGUMENTS

The Defendant, Telegram, argues that the interim order already in place, requiring Telegram to remove infringing channels, is sufficient to protect the Plaintiffs' interests. It's emphasized that Telegram can only disclose subscriber information if a court order designates someone as a terror suspect, citing their Privacy Policy. The

[23] Neetu Singh v. Telegram FZ LLC, 2022 SCC OnLine Del 2637.

Information Technology Intermediary Guidelines and Digital Media Ethics, 2021, was also referred to, which dictate the conditions under which subscriber information can be disclosed. Telegram's servers are in Singapore, and they adhere to Singaporean law, which means that disclosure of information can only occur under Singaporean court orders.

REASONING

Telegram acknowledges the Plaintiffs' copyright and has taken measures to block infringing channels. However, it resists disclosing user data due to Singaporean law and the server location. It asserts intermediary status under Indian IT law and cites Section 72A of the IT Act if forced to disclose user data. The Plaintiffs seek disclosure of channel creators' identities to combat concealed infringing channels. Telegram emphasizes content removal efforts and concerns about freedom of speech if the new channel feature is disabled. It stores data on encrypted cloud servers, follows privacy policies, and shares data with safeguards. Telegram's Privacy Policy addresses copyright infringement for public content. Data centers are in different jurisdictions, with data disclosure to authorities on court orders due to terrorism suspicions. The lawsuit aims to prevent copyright infringement of course material, videos, and tutorials. The court's jurisdiction is valid since the Plaintiffs reside and operate in Delhi, where the infringement has occurred, even if infringers use Telegram. Plaintiff No.1's materials fall under the Copyright Act's "literary works" and "cinematographic films" categories, with exclusive rights for copyright owners. Telegram's distribution constitutes "communication to the public" and infringing copies under the Copyright Act's definitions.

DECISION

Telegram's data center location in Singapore does not exempt it from Indian court orders due to its popularity and the infringement's Indian nature, under Indian jurisdiction. Singapore's PDPA has exceptions for data privacy in cases of copyright violation, allowing disclosure. Privacy and freedom of speech cannot justify non-disclosure for illegal actions. Telegram's reliance on Indian IT Guidelines doesn't excuse it from protecting intellectual property rights under the Copyright Act. Section 81 of the IT Act clarifies that the IT Act supplements the Copyright Act.

Thus, the Singapore server location doesn't render copyright owners powerless against infringers, especially when seeking legal remedies.

b. Jaydeep Madhukar Wakankarv. State of A.P.[24]

FACTS

Two criminal petitions seek to quash proceedings initiated under the Information Technology Act, 2000 and the Indian Penal Code, 1860. The proceedings stem from a complaint by M/s. Mahathi Software Pvt. Ltd. (Respondent No. 3). On May 14, 2021, Allscripts Healthcare, LLC, abruptly terminated the MOU signed with Respondent No. 3 with a notice on the 14th May 2021, thereafter it breached the privacy of the complainant Company by illegally accessing the servers and removed the subscription and potentially confidential data and further disabled administrative access of complainant's to its own Azure Tenant from the Complainant's office at Vizag by obtaining global admin privileges to Complainant's tenant, for illegal gains. Then Respondent No.2 i.e., Cyber Crime Police filed against eight accused under Sections 43[25], 65[26], 66[27], 66-B[28], 66-C[29], 66-D[30] of the IT Act, 2000, and Section 204[31], 120[32] of IPC, 1860. The petitioners argue that this complaint is retaliatory and baseless. They claim the complaint lacks merit as they were not properly implicated in the case and cannot be held liable for the actions of the company.

ISSUE

The key issue is whether the criminal proceedings initiated against the petitioners should be quashed based on the allegations of retaliation and improper naming of the accused.

PETITIONER'S ARGUMENTS

[24] Jaydeep Madhukar Wakankar v. State of A.P., 2022 SCC OnLine AP 3278.
[25] Penalty and compensation for damage to computer, computer system, etc.
[26] Tampering with computer source documents.
[27] Computer related offences.
[28] Punishment for dishonestly receiving stolen computer resources or communication device.
[29] Punishment for identity theft.
[30] Punishment for cheating by personation by using computer resources.
[31] Destruction of documents to prevent its production as evidence.
[32] Concealing design to commit an offence punishable with imprisonment.

The petitioners contend that the complaint is retaliatory, as it is in response to U.S. litigation. They argue that the charges do not meet the requirements of the sections mentioned in the charge sheet. They also claim that they cannot be held liable for the company's actions without the company being named as an accused.

RESPONDENT'S ARGUMENTS

The prosecution alleges that the Indian entity is financially controlled by the U.S. parent company, making it a single entity. They assert that the accused were involved in tampering with and stealing intellectual property and have evidence to support their claims. The prosecution argues that the criminal complaint is not a response to the ongoing civil proceedings in the U.S. They also claim that the petitioners deleted or tampered with evidence to conceal their involvement in the alleged crimes.

REASONING

The investigation concluded that the accused had conspired to steal the source code and confidential data owned by Mahathi Software without proper authorization. Several individuals conspired to access and delete data from Mahathi Software Pvt. Ltd. The court considered the financial relationship between the Indian entity and the U.S. parent company and found that the Indian entity lacked financial autonomy. The court also considered the evidence provided by the prosecution (Complainant), including emails and deleted data, indicating the involvement of the accused in the alleged crimes.

DECISION

The court denied the petitioners' request to quash the proceedings. Instead, it suggested that they file a discharge application if they believe the charges against them are false. The court instructed the trial court to expedite the processing of any discharge applications.

IV. Conclusion

While India has made significant strides in framing regulations to address the challenges IT Act, 2000, SPDI Rules, 2011, and the recently enacted Digital Personal Data Protection Act, 2023, serve as a foundation for the regulatory framework. However, a more cohesive and streamlined

approach is necessary to ensure comprehensive protection of data and to foster a conducive environment for cloud service providers.

The GST regulations need to be revisited to provide clarity on the taxation of cloud services, eliminating ambiguities that may hinder the growth of the sector. Intellectual property laws also need to adapt to the nuances of cloud computing, especially concerning data ownership and protection of digital assets. Harmonizing these laws with international standards, particularly those emerging from the EU, China, and the US, will facilitate global interoperability and strengthen India's position in the global cloud ecosystem.

To address data localization requirements, India should strike a balance between safeguarding data security and promoting international collaboration. Learning from legal precedents in jurisdictions like the EU and the US can guide the formulation of effective legal frameworks. Cybersecurity and privacy laws, as seen in China, can be a source of inspiration for enhancing India's cybersecurity posture.

To foster innovation and collaboration, the government should consider incentives for compliance with international standards, creating a competitive advantage for businesses. Regular updates to these regulations in response to technological advancements will ensure their relevance and effectiveness in the dynamic field of cloud computing.

A collaborative effort between government bodies, industry stakeholders, and legal experts is imperative to address the existing challenges comprehensively. By doing so, India can position itself as a global leader in cloud computing, providing a secure and conducive environment for businesses and individuals alike.