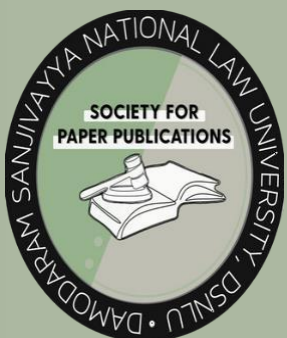
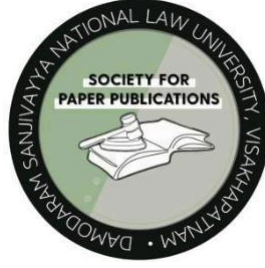




VOL 1, ISSUE III | OCTOBER 2023

Damodaram Sanjivayya National Law Journal





EDITORS

Sri Vaishnavi. M. N.

Ananya Panicker

Ayushman Somani

Teesha Seth

B. Solomon Raju

Veer Mahitha Kamireddy

Navya Kachroo

P. Sowmya Sri

Jawali Vuddagiri

Devanshi Pandey

Shaik Kousar

Dhanvin Pulavarthi



DAMODARAM SANJIVAYYA NATIONAL LAW UNIVERSITY

Nyayaprastha, Sabbavaram, Visakhapatnam 531035,

Andhra Pradesh, India

Published by
Dr. P Jogi Naidu
The Registrar,
Damodaram Sanjivayya National Law University,
Nyayaprastha, Sabbavaram

Visakhapatnam - 531035

Andhra Pradesh

India



Second Edition

October 2023

No part of this e-journal may be reproduced or copied in any form or by any means (graphics, electronics or mechanical), or reproduced on any information storage device for commercial purpose, without the written permission of the publishers.

Disclaimer: The views and opinions expressed in these papers and articles are those of the authors and do not necessarily reflect the official policy or position of the University or any other related authority. Assumptions made in the analysis are not reflective of the position of university other than the authors. Since we are critically thinking human beings, these views are always subject to change, revision and rethinking at any time. Please do not hold us to them in perpetuity.

Note: Due care has been taken while publishing the E-journal but the authors, editors, publishers, and printers are not responsible in any manner for any mistake that may have inadvertently crept in. Any mistakes noted may be brought to our notice that shall be taken care in the next edition. All disputes subject to Visakhapatnam jurisdiction only.



DAMODARAM SANJIVAYYA NATIONAL LAW UNIVERSITY

~a cradle of future jurists~


Prof. (Dr.) P. Sree Sudha, Ph.D. (Law), LL.D. (NLSIU)
Vice-Chancellor (Officiating)

FOREWORD

AI, robotics and other forms of smart automation have the potential to bring great economic benefits - up to \$15 trillion to global GDP by 2030 - causing a major shifting the global economy. It is seen as a key driver and component of the Fourth Industrial Revolution. This Revolution is more transforming than any other industrial revolution we already experienced so far. It challenges our ideas about what it means to be 'human'. The influence of AI can already be seen on the labour market (e.g. robotisation of work) as well as in public (e.g. facial recognition) and private spaces (e.g. virtual assistants at home). The integration of AI within our daily routines makes it hard to imagine life without it. Artificial intelligence (AI) is becoming increasingly more prevalent in our daily social and professional lives. AI can be of benefit to a wide range of sectors such as healthcare, energy consumption, climate change and financial risk management. AI can also help to detect cyber security threats and fraud as well as enable law enforcement authorities to fight crime more efficiently. AI systems are more accurate and efficient than humans because they are faster and can better process information. They can perform many tasks 'better' than their human counterparts. Companies from various economic sectors already rely on AI applications to decrease costs, generate revenue, enhance product quality and improve competitiveness. AI systems and robots can also have advantages for the specific sector in which they are to be used. While AI can make enforcement and adjudication more effective, potentially reduce discrimination, and make the drafting of contracts, briefs, laws, regulations, and court opinions faster and less costly, it also has serious implications for broad societal issues such as consumer protection; investor protection; false advertising; privacy; misinformation; and discrimination and civil rights.

There are also several important ethical issues associated with (programming and using) AI systems. The commercialisation of AI will pose several challenges from a legal and regulatory point of view as well. In this journal scholars from various legal disciplines critically examine how AI systems may have an impact on law. While specific topics of Indian law are thoroughly addressed, the journal also provides a general overview of a number of regulatory and ethical AI evolutions and tendencies in India. The journal additionally explains basic AI-related concepts such as machine learning, robots, Internet of Things and expert systems.

I thank the authors for their contributions and for their commitment in presenting their work in the form of articles, the reviewers for investing time and effort into analysing and providing valuable comments and corrections, and last but not least, the editorial team for managing the review and publication process efficiently and thoroughly. I hope that the selected publications will have a lasting impact on the academic community and that they will be motivating factors for other researchers to pursue their research goals.


P. SREE SUDHA

(University established by Govt. of A.P. Legislature Act No.32 of 2008)

"NYAYAPRASTHA", Asakapalli (V), Sabbavaram, Visakhapatnam - 531 035, Andhra Pradesh, INDIA
e-mail: vc2dsnlu@gmail.com, M: 9493425612, Fax No.08924-248213, Website: www.dsnlu.ac.in

TABLE OF CONTENTS

1. AD TARGETING: A SEEMING ATTACK ON DATA PRIVACY	6
2. THE INTERPLAY BETWEEN CONSUMER PROTECTION ACT 2019 & INFORMATION TECHNOLOGY ACT 2000: HAS IT BEEN EFFICACIOUS IN PROVIDING A SAFE HAVEN FOR CONSUMERISM?.....	15
3. ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ARBITRATION: A PLETHORA OF TECHNOLOGY?	25
4. CENTRAL BANK DIGITAL CURRENCY: RENOVATING THE INDIAN FINANCIAL SECTOR.....	39
5. UNREGULATED EQUITY CROWDFUNDING IN INDIA: A NEED TO FILL THE VACUUM IN THE EXISTING REGULATORY FRAMEWORK.....	49
6. CRIMINAL LIABILITY OF ARTIFICIAL INTELLIGENCE.....	60
7. DIGITAL TRANSACTIONS AND THE RISE OF CYBERCRIMES: TESTING THE READINESS OF THE INDIAN LEGAL STRUCTURE	67
8. RESERVE BANK OF INDIA'S CENTRAL BANK DIGITAL CURRENCY (CBDC).....	84
9. FANTASY SPORTS AND ONLINE GAMBLING: A VIEW THROUGH LEGAL LENS	101
10. JURISPRUDENTIAL ANALYSIS OF LEGAL AND ETHICAL CONUNDRUM SURROUNDING ARTIFICIAL INTELLIGENCE	110

ADVERTISEMENT TARGETING: A SEEMING ATTACK ON DATA PRIVACY

-Harshit Adhikari & Falguni Mundhra¹

I. INTRODUCTION

“Privacy is not an option,

And it shouldn't be the price we pay just for getting on the internet.”

Our world is filled with all sorts of people. Some good and some bad. there are always those who wish to take advantage of us and benefit from it. Are we comfortable with sharing all our information with strangers? If not all of it then exactly how much are we willing to share? Are we really in control of the amount of information that is available to others?

Everyone has things that they wish to keep to themselves, be they physical or maybe even digital. The fear of the consequences of these things being exposed to unwanted entities is why everyone values privacy and security so much in the case of both, physical and digital matters.

We live in the digital era, the era of data. Data is the oil of the modern world.² We want our data to be used only for our benefit, we want it to enhance our digital experience but not for causes that will harm us. Some amount of our data being accessible to the government is a necessity for matters of national security. But there should be a limit to that and there should be measures to ensure that these limits are not exceeded. But there are always people who wish to exploit others for their own gain. We see regular evidence that there are possibilities of our data being exposed or misused by different entities. Hence the current worldwide rage about data privacy. Data privacy in a general sense refers to the ability of the user to control the extent to which their personal information is made available to or communicated to others. The data in question can be the user's identity, location, contact information, or information regarding behaviour on the internet.

¹ The authors are students in their II year at KIIT school of law, Odisha.

² Stephen J. Biglew, Data Privacy (Information Privacy), TechTarget, <https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy>

II. IMPORTANCE OF DATA PRIVACY IN THE MODERN AGE

Now more than ever before we need the ability to handle data. The modern world is pacing toward digitization. There is an overflow of data. With that, there is an increase in the need to be able to keep this data secure and private. We are striving our hardest to have all sorts of processes and documents available online this increase in usage of the web has increased the importance of data privacy. Companies behind applications, social media, and websites collect data about us to be able to provide services to us. The govt. and these private corporations that collect our data claim to be using it for good purposes like ensuring the security of our nation or things like better experiences in the digital world. But how can we be sure of that? Remember the last time you talked to a friend about something and an ad for it popped up on your browser? A few times and it could have been a coincidence but the sheer frequency is what scares people and makes them doubt the words of the big data companies.

We have seen many cases where someone's data is compromised and they are blackmailed to not have their data revealed to the general public. Sometimes these incidents include information like bank details which cause huge financial losses. These create doubts in people's minds and cause them to refrain from engaging online. People need assurance that their privacy is ensured to feel safe in online activities. Organizations need to show people the several steps they are taking to ensure data privacy so that people trust them with their data.³

There are various ways our data can be misused after a breach in its security or if people do not possess the ability to control the way their data is stored or used:

- There can be harassment or fraud faced by users through the hands of criminals

³ CLOUD FLARE, What is Data Privacy?, <https://www.cloudflare.com/learning/privacy/what-is-data-privacy/#:~:text=Data%20privacy%20is%20also%20important,trusted%20with%20their%20personal%20data.>

- Entities can sell the private data of users to advertising agencies so that the user receives unnecessary marketing or advertisement
- The tracking of individual's activities can lead to limited expression of opinions and limited online activity, especially in places where the govt. is repressive.

The level of privacy that we are afforded right now is not desirable enough for a lot of people. Some companies still do not place adequate security measures around the data they collect from gullible users in the name of better services. The lack of said security may lead to a breach which can lead to compromise the privacy of the users.

Does it not become scary when the internet seems to know things about us that we did not share?

III. A SEEMING ATTACK ON DATA PRIVACY i.e. TARGETED ADS

Sometimes the type/amount of data being collected exceeds our expectations. How many times have you opened your social media and come across an advertisement for a product your friend told you about? Even though we never searched about it, we got ads about it. We get ads of things that we heard at some event. How does that happen? Are our devices listening to us? If not, then how do these advertising companies find out? Sometimes we get advertisements about things we just happened to think about, we get these ads without even talking about these things. Do these companies know so much about us that they can guess the kind of things we might like or the things that might be the subject of our conversations? Would that not require them to know our friends, their interests, and their backgrounds as well? Even the sources mentioned above would not allow companies to understand us so thoroughly. Do these companies really have access to so much information about us? The unfortunate answer to this question is YES.

Advertising companies realized that since random advertisements are everywhere, the general public has gotten pretty good at ignoring them. This has forced advertising agencies to take a few steps to generate and provide us with ads that we are most likely to engage with. These ads focus on our specific traits, interests, and our preferences. The advertisers discover these after tracking our activities on the internet.

Let's say we search for a CD of your favourite band on the internet, the website on which you look for it, uses it to store cookies on your device which tells the other websites, that you visit in the future about your preference which then use it to show you advertisements which are as similar as possible to the object you were looking for i.e. they may show you ads for T-shirts of the same band or CDs of some other similar band.

Aside from cookies, advertisement companies also learn about us in different ways like checking our search engine history and they even try to find our personal information from social media. These ads target us across different devices as well, these make it seem like nothing we do is private, these companies use all their means to find out about our age sex religious relationship status, etc. to give us ads that are as relevant to us as possible.

These advertisements that we get after our data is revealed to different entities, are called targeted advertisements. To make the practice of targeted advertisements seem more ethical the websites or services we use give us an option on whether we would like to store cookies or not, but is it really an option? We can disagree to store cookies but then we would be unable to use the necessary website application or any other facility. Simply said we are bound to accept these cookies.⁴ We need to be able to access all our necessary websites without being forced to give permission to unknown entities to access information about us. The fact that we are being forced to accept giving up our data by our own hands because of a subtle threat from these huge data companies should be alarming to us all. Those who find this alarming have been demanding government intervention in these areas for a long time. We need proper laws and mechanisms to feel safe on the world wide web because ensuring proper security and data management is the only way to get more people to interact online and go about their activities without feeling heavily restricted.

IV. LAWS RELATING TO DATA PRIVACY

There exist several legislations dealing with information technology, contracts, intellectual property, and criminal acts, that ensure our security, offer protection, and impose civil and criminal responsibility, but even today in this modern era where data is everything, India does not have a single, comprehensive law that protects privacy or personal data. Currently, India's

⁴ AMLEGALS, Targeted Advertisements- An Invasion Of Privacy?, accessed on 15.01.2023, <https://amlegals.com/targeted-advertisements-an-invasion-of-privacy/#>

legal foundation for data protection and privacy is provided by the rules laid under the Information Technology Act, 2000 ("IT Act"). The very thought of sensitive private data is discussed through these laws.

In addition to suggesting that privacy laws be established, the Justice Shah Report on Privacy in 2012 identified 57 particular sectoral and policy recommendations that already exist that have ramifications for privacy and must therefore be changed as soon as the new legislation is passed.⁵ While the personal data protection bill is pending in the parliament, there are other acts and provisions that govern the data privacy matters, such as,

1. Constitutional Protection

Such a supposedly restricted right to privacy has received the utmost priority from Indian courts, who believe that it may only be curtailed for compelling grounds like public safety and national security.⁶ Although a challenge was accepted in 2015, the Apex Court of India has decided in 2018 that the right to privacy is, definitively, a basic right protected by the Constitution.⁷ It is important to remember that the privacy of humans has been acknowledged as a basic right and is protected by several international human rights agreements.⁸

2. Information Technology Act, 2002 and Privacy Rules

The IT Act aims to safeguard electronic data, including non-electronic documents and information that have been, are being, or will be handled electronically. It contains relevant provisions for collecting, transferring and using personal data. According to the Privacy Rules⁹, businesses that collect, handle, and store personal data should be monitored to check if they properly follow rules regarding such handling of our data including sensitive personal information. As a subset of personal information, it differentiates between “personal information” & “sensitive personal data or information” (“SPDI”).

⁵ Justice A. P. Shah, *Report of the Group of Experts on Privacy*, Planning Commission of India (2012), <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf>

⁶ *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

⁷ *Puttaswamy v. Union of India*, (2017) 10 SCC 1.

⁸ G.A. Res. 217 (III) A, Universal Declaration of Human Rights (1948).

⁹ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, MINISTRY OF COMMUN. & INFO. TECH., GOV'T OF INDIA, <http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>

3. Indian Contract Act, 1872

Under the Contract Act, one can get damages or compensation for the violation of any terms under the contract which may include one's privacy and also for not performing the promise made under the contract, including those which are connected to data expressly or not obligating the rules by breach of contract.

4. Criminal Laws – Indian Penal Code, 1860

Theft, misappropriation of property, and criminal breach of trust are all crimes that can be prosecuted in cases when data is stolen. For instance, the dishonest theft or conversion of another person's "movable property" for one's use is punishable by law under section 403 of the IPC.¹⁰ The penalty for such criminal violations, like a breach of trust, is severe and includes a fine, a term of imprisonment up to 3 years, or both.

5. Intellectual Property Laws – Copyright Act, 1957

Rights in literary, theatrical, musical, artistic, and cinematic works are governed by the Copyright Act of 1957 in India. In accordance with this Act, Indian courts have recognised the copyright in computer databases¹¹ & given them the status of "literary work." Depending on the seriousness of the offence, the Indian Copyright Act imposes obligatory penalties for copyright violations. According to Section 63B of the Indian Copyright Act, anybody found guilty of intentionally making an illegal copy of a computer program by using a computer faces a minimum jail sentence of 6 months and a maximum sentence of 3 years.

6. Credit Information Companies Regulation Act, 2005

The Credit Information Companies Regulation Act ("CICRA") has established a stringent framework for safeguarding information on the credit and finances of individuals and businesses in India. It is based on the Fair Credit Reporting Act and Graham Leach Bliley Act. The CICRA mandates that the credit information of Indian citizens be gathered in accordance with the privacy standards outlined in the CICRA rule. Regulations under CICRA, which have been announced by the Reserve Bank of India, set forth strong data privacy norms.¹² Any potential breach or change of this data is the responsibility of the organisations collecting and storing it. The following organisations are listed in the regulations as "specified users" who fall under the jurisdiction of the CICRA and are permitted to gather credit information.¹³

¹⁰ INDIAN PENAL CODE, 1860, §403.

¹¹ Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, (1996) 113 PLR 31.

¹² Credit Information Companies Regulations, 2006 Under Section 37 of the Credit Information Companies (Regulation) Act, 2005, MINISTRY OF FINANCE, DEPT. OF ECONOMIC AFFAIRS, BANKING DIVISION, GOV'T OF INDIA, <https://rbidocs.rbi.org.in/rdocs/Content/PDFs/69700.pdf>

V. THE NEED FOR DATA PRIVACY LAWS

It is extremely essential to pass a particular privacy and data protection law as a starting point. So that it is not necessary to control private companies like Facebook or Google. It basically claims that if the consumer is having or is concerned with the issue of privacy while using any particular application then he/she will change their behaviour towards the application. These changes could be restricted use of the application or stopping the use altogether etc. such changes in consumer behaviour would drive businesses to provide better privacy safeguards. Users frequently have less knowledge than data controllers regarding the scope of data collection, how it is processed, shared, and used, as well as the implications of sharing this data with others or incorporating it into an algorithm.¹⁴ This is known as information asymmetry. In reality, consumers rarely receive any kind of notification when and if their information is shared with other parties. Researchers have discovered that consumers frequently consider privacy policies as promises of data protection, rather than just liability disclaimers for businesses, or that the mere existence of a privacy policy, independent of its contents, is viewed by the general public as a substantial privacy safeguard.¹⁵

The 2018 Draft Data Protection Bill, which was suggested by the Committee of Experts led by Justice Srikrishna, is a positive development. Taking into consideration international trends like the implementation of the “European Union General Data Protection Regulation (GDPR)” as well as the Supreme Court's “privacy ruling in Puttaswamy”, it has participated in public dialogue and aided in the advancement of the discussion on privacy and data protection.¹⁶ The cloud method is increasingly being seen by EU legislation as a “method reasonably expected to be utilised” and as making more information “identifiable”. In

¹³ *Id.*, Rule 3.

¹⁴ Acquisti, Alessandro and Jens Grossklags, 'What Can Behavioral Economics Teach Us about Privacy', *Digital Privacy: Theory, Technologies & Practices*, 2007, Pp.363.

¹⁵ Tene, Omer and Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, Stanford Law Review Online, 2012, 65.

¹⁶ Vrinda Bhandari, *PRIVACY CONCERNS IN THE AGE OF SOCIAL MEDIA*, India International Centre Quarterly, Vol. 45, No. 3/4, Social Media in a Networked World (Winter 2018-Spring 2019), pp. 78.

addition, different dangers are connected to data that may be linked to an identifiable person rather than information that is currently attached to an identified person.¹⁷

While in India, in *People's Union for Civil Liberties v. Union of India*¹⁸, the Supreme Court noted that data sharing promotes the right to knowledge of a voter or citizen. The right to privacy of an individual must be given priority over the right of people to information when their interests conflict because the former serves a greater good. The issue of a voter's right to know about a candidate's privacy is raised. It calls for a balanced interest and attitude. Therefore, communal good and individual liberty must finally have a healthy and cordial connection.¹⁹

VI. CONCLUSION

The issue of implementation comes first. India has a limited state capacity, as seen by its poor ability to enact effective laws and enforce them. To ensure the effectiveness of the laws, certain things need to be ensured. Firstly, the grievance redressal method must be efficient and user-friendly. The capacity to guarantee the Data Protection Authority's (or any other ombudsman's) financial and functional independence, which is planned to be established under the Draft Bill of 2018, must be second and related. The third more significant concern should be about how the laws may unintentionally strengthen the monopoly of current firms by making it more difficult for new competitors to enter the market.²⁰ When evaluating the effects of the loss of our privacy caused by actions taken by the government as well as private entities, all these elements need to be taken into consideration. In the world we live in, technology will always advance faster than the law. Today, big data has given the government and commercial businesses the ability to build detailed profiles of citizens and individuals, giving them tremendous power to conduct surveillance or make important choices that directly affect people's lives.²¹ Through the public discussion of the Srikrishna Committee Report and the 2018 draught Data Protection Bill, we as a nation have moved in the right direction towards ensuring a more secure and less restrictive digital world.

¹⁷ Schwartz & Solove, Council Directive 95/46, at 1841-45 (explaining how individuals can be re-identified by putting together various pieces of de-identified information).

¹⁸ AIR 2003 SC 2363

¹⁹ Shiv Shankar Singh, PRIVACY AND DATA PROTECTION IN INDIA: A CRITICAL ASSESSMENT, *Journal of the Indian Law Institute*, October-December 2011, Vol. 53, No. 4, pp. 670.

²⁰ *Supra* note 12.

²¹ *Id.*, at 79.

**THE INTERPLAY BETWEEN CONSUMER PROTECTION ACT 2019 AND
INFORMATION TECHNOLOGY ACT 2000: HAS IT BEEN EFFICACIOUS IN
PROVIDING A SAFE HAVEN FOR CONSUMERISM?**

-Vanshika Srivastava¹

ABSTRACT

Consumerism along with the interests and rights of consumers, has gained an enhanced significance in the era of digital economy. Providing a well-established legal framework for protecting the interest of public is of paramount importance for every governmental or non-governmental entity. The enactment and introduction of the Consumer Protection Act, 2019 and its subordinate Consumer Protection (E-commerce) Rules, 2020, has been a paradigm shift in this direction. This legislation efficiently aimed at filling the vacuum that existed in the Consumer Protection Act, 1956, with respect to the rights and interests of consumers and the duties and liabilities of business entities in the digital space. The advent and exponential growth of digital economy requires that adequate safeguards should also be duly incorporated in the laws of the country.

Interestingly, the Information Technology Act, 2000, also aimed at augmenting the growth of e-commerce and digital economy in the country. While it has shown remarkable progress in some aspects, it still fails to establish trust between traders and consumers in the online space. It is this mutual trust and confidence which forms the bedrock of digital economy and is instrumental for the growth of e-commerce industry.

This article has closely analyzed various dimensions of the interplay between the Information Technology Act, 2000 and the Consumer Protection Act, 2019. It has further focused upon understanding the effectiveness of the legislations regarding the protection of consumerism in the current scenario and recent legal developments in this field.

¹ The author is in their 3rd Year at National Law Institute University, Bhopal.

I. INTRODUCTION

Digitalization has not left any aspect of human life untouched in the current scenario. There have been active efforts from all across the globe to incorporate digitalization, so as to keep pace with the rapid developments and advancements in the space of information technology. The situation is no different in India wherein a flagship initiative was launched by the Central Government to digitalize the country under the 'Digital India' program². The advent of the digital era has been marked by the promising growth of digital economy in India. The market of commercial and business activities has witnessed immense growth and enhanced experience with the commercialization of activities.³ E-commerce transactions offer multiple benefits both to the business entities and the consumers. Its unique features such as unboundedness, multiplicity and virtuality allow the exchange of goods and services across the globe, without any physical and time constraints. These features have contributed immensely to the growth and flourishing of e-commerce in India and around the world, however, e-commerce activities pose several challenges too. Threats to data protection and privacy, data integrity and security, lack of loyalty in consumer relations and threat to the violation of consumers rights in the digital space, form variety of challenges which plague the arena of e-commerce.⁴

Ensuring adequate safeguards for protecting the rights of consumers in the e-commerce transactions has gained significant importance. If online commercial transactions are not regulated stringently with regards to the interests of consumers, it may eventually lead to dire consequences, such as adverse impact on fair competition and free flow of authentic information in the system. This would further lead to deception and fraud on consumers, which would amount to flagrant violations of their rights. India has made several attempts to holistically guarantee and protect consumer rights through slew legislations. Various enactments aim at dealing with different aspects involved in e-commerce transactions and consumer protection. The two leading legislations currently in this field are the Information

² *Digital India program*, <https://digitalindia.gov.in/>

³ Rajiv Khare & Gargi Rajvanshi, *E-commerce & Consumer Protection: A Critical Analysis of Legal Regulations*, CLAP NLS, 55, 56-57 (2021).

⁴ Veeramani Siv, *Consumer Protection in the Age of Digital Transformation: A Judicial Response in India*, ICME, 137, 140-141 (2019).

Technology Act, 2000⁵ and the recently enacted Consumer Protection Act, 2019⁶ and its subordinate Consumer Protection (E-commerce) Rules, 2020.⁷

II. NEED FOR CONSUMER PROTECTION IN THE DOMAIN OF E-COMMERCE

Commercial organizations are well organised and structured institutions which are well informed and enjoy a better dominating position than the consumers in the market. This places the consumers in a position which renders them vulnerable to exploitation at the hands of the commercial entities. This was categorically noted by the apex court in *Indian Oil Corporation v. Consumer Protection Council*⁸, wherein it held that the worst affected victims of these commercial organizations are the consumers and they need to be duly protected through the consumer protection. The consumers all across the globe enjoy multiple rights now, however, all these rights emanate from the four basic rights that were propounded by the former President of United States of America, Mr. John F. Kennedy, while he introduced the “*Bill of Consumer Rights*” in Congress in 1962. The four rights laid down by were-

- i. Right to Safety,
- ii. Right to Information,
- iii. Right to Choice,
- iv. Right to be Heard.

The advent of Information and communication technology has introduced fundamental changes in commercial and business transactions. The use of internet has propelled businesses to reach great heights at global platforms. However, this dynamic shift has exposed the consumers to innumerable threats, the most prominent of them being-

- i) Exposure to unfair trade practices, ii) Insufficient information disclosure, eg., refund policies, information regarding warranty, cancellation terms⁹, etc., iii) unsafe products, iv) lack of confidentiality of consumer’s information, v) protection of identity of seller, vi) goods delivered fail to correspond to the description, quantity and quality, vii) Data privacy violations, viii) insecure payment mechanisms, etc.

⁵ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

⁶ Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).

⁷ Consumer Protection (E-commerce) Rules, 2020, The Gazette of India, 2020 (India).

⁸ *Indian Oil Corporation v. Consumer Protection Council*, (1993) 1 SCC 397.

⁹ Neelam Chawla, *E-Commerce and Consumer Protection in India: The Emerging Trend*, JOURNAL OF BUSINESS ETHICS, 581, 581-582 (2020).

The presence of such loopholes in the arena of e-commerce can potentially hamper the growth of this model. Hence, there existed a pressing need for developing and executing a robust legal framework for catering the needs of the evolving society.

III. CONSUMER PROTECTION IN DIGITAL ERA: LEGAL FRAMEWORK IN INDIA

There exist several legislations which address different aspects involved in E-commerce and Consumer Protection, however, the Information Technology Act, 2000¹⁰ and the recently enacted Consumer Protection Act, 2019¹¹ and its subordinate Consumer Protection (E-commerce) Rules, 2020¹² have gained prominence.

1. Information Technology Act, 2000

The conduct of commercial transaction over electronic media requires a stringent regulatory framework to prevent the multitude of wrongful and illegal acts that can very conveniently be carried out in the digital space, under the garb of anonymity. Thus, the online space and the protocols to be followed which operating in the online space precisely catered by the Information Technology Act, 2000. The relevant provisions have been analysed hereunder-

- The issues concerning Consumer's exposure to unfair trade practices have not been categorically dealt with in this Act, however, it goes a long way in tackling the issues which intermingle with the same.
- Section 6A of the Act mandates the concerned service provider to deliver its services in the most efficient manner¹³. It provides no room for procedural lapses which could be easily avoided by the efforts of the service provider.
- Section 8 of the Act provides that the law and provisions which are related to the regulation of IT transaction should be duly published in the Official Gazette¹⁴. This provision aims at bringing the provisions and laws to the notice of the public and creating awareness in them. Thus, it leads to the propagation and dissemination of authentic information which goes a long way in protecting and informing consumers.¹⁵

¹⁰Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

¹¹Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).

¹² Consumer Protection (E-commerce) Rules, 2020, The Gazette of India, 2020 (India).

¹³Information Technology Act, 2000, § 6A, No. 21, Acts of Parliament, 2000 (India).

¹⁴Information Technology Act, 2000, § 8, No. 21, Acts of Parliament, 2000 (India).

¹⁵ Priyanka Barik, *Cyber Law's Emerging Role in Indian E-commerce*, <https://ksandk.com/regulatory/indian-e-commerce-law-under-cyber-law/> KING STUBB & KASIVA (Dec 25th, 2022).

- Section 10 of the Act provides legal validity to the contracts which are entered into on the electronic medium. This enables the parties to the contract to legally enforce the contract and sue on breach of contractual obligations.
- Chapter V – Section 14-16¹⁶ of the IT (Amendment) Act, 2008, provides that the transactions conducted in the electronic medium would be treated as secured transactions and payment mechanisms. This security instils trust and surety in the minds of the consumers.
- Section 72 & 72-A¹⁷ of the Act addresses the penalty that one would incur in case of a potential breach of privacy and confidentiality. This provides safety and security to the parties involved.
- Section 66D¹⁸ of the Act does not make it necessary for the seller to reveal his identity to the buyer, however, it entails a penal punishment of a specified term of imprisonment and fine, if the seller wrongly impersonates himself and cheats the buyer.

2. The Consumer Protection Act, 2019

Until 2019, the primary legislation that dealt with the rights and interests of the consumers has been the Consumer Protection Act, 1986. However, this Act proved to be incapable at effectively handling the complex situations which started emerging with the advent of the digital era. It lacked the framework of tackling the issues which revolved around e-commerce and related aspects. Thus, the legislature enacted the Consumer Protection Act, 2019 ('New Act') in 2019 to comprehensively address the issue of consumer protection. This new act has traversed a long way in protecting the interests and rights of the consumers in digital transactions and e-commerce activities. Some of the most significant provisions of this Act have been discussed below-

- The first and foremost development towards bringing e-commerce under the regime of consumer protection was expanding the definition of consumer under the New Act. Section 2(7) of the Act defines consumer to be a person who “buys any goods” and “hires or avails any services”¹⁹. This includes any online or offline services through transactions and electronic means. This enlargement of scope benefits the consumers in online space being providing inclusivity.

¹⁶Information Technology Act, 2000, Chap. 5 § 14, No. 21, Acts of Parliament, 2000 (India).

¹⁷Information Technology Act, 2000, § 72, No. 21, Acts of Parliament, 2000 (India).

¹⁸Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).

¹⁹Consumer Protection Act, 2019, § 2, cl. 7, No. 35, Acts of Parliament, 2019 (India).

- The New Act has also been bestowed with the definition of the term ‘*e-commerce*’. Section 2(16) defines ‘*e-commerce*’ as means of buying or selling of goods or services including digital products over digital or electronic network²⁰.
- Furthermore, the term ‘*electronic service provider*’ has been defined in Section 2(17) as any person who provides processes or technologies to enable a product seller to engage in advertising or selling goods or services to a person²¹. It includes online auction sites and any online market place.
- Section 2(47) of the Act has laid down stringent provisions wherein it has stated that if a service provider, merchant or trader reveals or shares the personal information of any consumer without their express consent then it would be categorically covered under the domain of ‘Unfair Trade Practice’²².
- Section 21 entails penalty provisions for any seller, trader, manufacturer, retailer or endorser, whoever perpetrates any false or misleading information through a misleading advertisement²³. Monetary Penalty can be imposed upon any such person who engages in such an activity and the Central Consumer Protection Authority is entrusted with the task of imposing the penalty.
- Chapter 4 Section 3-9 entails provisions to establish a Central, State and District Consumer Protection Council that would aim at providing advice and recommendation to the Government of the Country, State and District regarding enhanced protection of the consumer’s rights²⁴.
- Section 94 of the Act provides that the Union Government is empowered to take necessary steps to prevent unfair trade practices, direct selling and other vices involved in e-commerce transactions. The government can also prescribe rules in order to prevent unfair trade practices and fraud by e-commerce entities.

²⁰Consumer Protection Act, 2019, § 2, cl. 16, No. 35, Acts of Parliament, 2019 (India).

²¹Consumer Protection Act, 2019, § 2, cl. 17, No. 35, Acts of Parliament, 2019 (India).

²²Consumer Protection Act, 2019, § 2, cl. 47, No. 35, Acts of Parliament, 2019 (India).

²³Consumer Protection Act, 2019, § 21, No. 35, Acts of Parliament, 2019 (India).

²⁴Consumer Protection Act, 2019, Chap. 4 § 3-9, No. 35, Acts of Parliament, 2019 (India).

- Section 101 provides for the execution of the power that has been vested by Section 94 in the government. It provides that the Central Government can make rules, by notification²⁵ so as to give effect to the provisions of Section 94.

IV. THE EMERGENCE OF THE NEW ACT

The above-mentioned provisions saliently incorporate the protection framework that has been established under the New Act, to specifically cater to the commercial transactions in the digital space. Until the enactment of this piece of legislation the rights and interests of the consumers were being hampered and compromised as the Consumer Forums lacked the adequacy to redress issues in the current digital domain.²⁶ They were appropriately equipped to handle the cases that emerged in the most effective and efficient way.²⁷ This jeopardized the prospects of securing protection for the rights that the consumers should ideally be entitled to.²⁸ The sudden splurge in the e-commerce activities and the conduct of online transactions without sufficient protection mechanism for the rights of the consumers deterred them from actively participating in such transactions.

The intent behind including consumer centric provisions in the Information Technology Act, 2000, was also to lay down regulations and rules that would determine conduct in related activities in the digital space. It aimed at the growth and promotion of e-commerce and to establish trust between the consumers and online traders so as to create and promote a conducive environment for trade and transactions between the parties. However, both these legislations fell short on the techno-legal aspects and were plagued with several lapses. Then with the introduction of the Consumer Protection Act, 2019 and the subsequent Consumer Protection Ecommerce Rules, 2020, the rights of consumers have garnered the attention that it should receive and their interests are being given the requisite consideration which they demand.

²⁵Consumer Protection Act, 2019, § 101, No. 35, Acts of Parliament, 2019 (India).

²⁶ Rajiv Khare & Gargi Rajvanshi, *E-commerce & Consumer Protection: A Critical Analysis of Legal Regulations*, CLAP NLS, 55, 56-57 (2021).

²⁷ *Id.*

²⁸ *Id.*

V. JUDICIAL APPROACH TOWARDS THE PROVISIONS OF THE NEW ACT

Recent legal developments have clarified the stands adopted by the judicial and quasi-judicial bodies with regards to the application of the provisions of the new Act.

A vital judgement being the case of *Horlicks Ltd. V. Zydus Wellness Products Ltd.*²⁹, wherein Zydus in one of its advertisements while promoting its product 'Horlicks', depicted a comparison between its product and another rival product 'Complain'. The advertisement showed that their product was better and healthier than the rival product. The court held that the advertisement could not be saved under Article 19 1(a) of Constitution since it constituted to be an unfair trading practice, and it was ordered to bring down the impugned advertisement. The court further laid down that if any comparisons are being made, they should not directly mislead or disparage. The advertisement in dispute has the ability to deceive consumers and also show-cased a false competitive spirit.

The *Connaught Plaza Restaurants ltd. V. KapilMitra*³⁰, is another significant progress in this regard. The Mc Donald's franchise situated at Connaught Plaza Restaurants Ltd. had organised a contest wherein they assured the customers of winning a prize whenever they ate the restaurant. However, the terms and conditions of availing the gifts and the scheme were concealed from the customers who were denied the gifts. After winning the contest they were intimated about the extra mandatory purchases that they were supposed to make. The NCDRC claimed that the practice amounted to an unfair trade practice and ordered compensation for the complainant and all other customers who have been deceived by such a practice as it was of the nature of a misleading advertisement.

VI. ANALYTICAL VIEWPOINT- INEFICIENCIES OF THE LEGISLATIVE FRAMEWORK

The Consumer Protection Act 2019³¹(CPA) and the Information Technology Act 2000³² (IT Act) have both been enacted to protect consumer rights in India. However, there have been instances where these two acts have failed to work together effectively to protect consumerism in India.

²⁹*Horlicks Ltd. v. Zydus Wellness Products Ltd.*, 2020 SCC Online Del 873.

³⁰*Connaught Plaza Restaurants Ltd. v. Kapil Mitra*, 2020 SCC Online NCDRC 192.³¹

Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).

³² Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

One of the key areas where the CPA and the IT Act have failed to work together effectively is in cases of online fraud and scams. While there exists a strong legislative framework in this regard in the CPA, the IT Act does not specifically address online fraud and scams. This has created a gap in the legal framework, which cybercriminals have been able to exploit.

Another area where the CPA and the IT Act have failed to work together effectively is in cases of data privacy and security. While the IT Act has provisions for data privacy and security, the CPA does not specifically address these issues. This has left consumers vulnerable to data breaches and identity theft, which can have a significant impact on their lives. Furthermore, there have been instances where the IT Act has been used to curtail free speech and expression, which are essential components of consumerism.³³ In such cases, the IT Act has been misused to target individuals and organizations that have spoken out against companies and products, thereby undermining consumer protection.

In conclusion, while both the CPA and the IT Act are important laws for protecting consumer rights in India, there is a need for greater coordination and collaboration between the two acts to ensure comprehensive and effective consumer protection in the digital age.

VII. THE EXISTING LOOPHOLES AND THE WAY FORWARD

The new Act seeks to criminalise certain acts such as unfair trade practices, insufficient information disclosure, data privacy violations, etc. which seriously hamper the rights of the consumers. It has expanded the jurisdiction of the quasi-judicial bodies and the Commissions and forums to deal with the issues which emerge out e-commerce transactions. Still certain vital issues continue to exist, like the prevalence of the ill effects of the highly competitive marketplace wherein the same products might be sold by different vendors at starkly different prices, thereby making it difficult to assess the true worth and value of the product.

Although provisions have been incorporated in the new Act to deal with privacy and data protection issues yet risk of potential misuse of data and personal information exists. Furthermore, concerns such as hacking, computer fraud, virus and alteration of financial

³³ *Section 66A of the IT Act, 2000*, LEGAL SERVICES INDIA, <https://www.legalserviceindia.com/legal/article-1905-section-66a-of-the-it-act>.

information, interception³⁴ are issues which have not been categorically and specifically dealt with in the legislations. Moreover, the entire consumer protection regime needs to be strengthened and better equipped so that justice is delivered to the consumer whose interests have been hampered or who have fallen prey to the vices of the business entities and its conduct. Efforts need to be made to educate consumers about their rights and rigorous implementation of them at every forum.

VIII. CONCLUSION

In the current global conditions, a strong, fair, competitive and progressing market can only sustain if the rights of the consumers are duly protected and recognised. Since consumers form the backbone of the entire commercial business system, safeguarding their interests becomes of utmost importance. The encounter of law and technology creates excellent opportunities but also poses several threats to the business world. The advent of e-commerce in India was a turning point both for consumerism and for the business entities. While the traders and sellers witnessed booming growth in their business consumerism on the other hand were witnessing several threats and challenges to their interests. India gravely lacked in creating a sustainable and comprehensive framework for protecting the rights of consumers until 2019. The Information Technology Act, 2000 has provided significant guidance in the e-commerce regime and regulated the activities in this domain until the revamped legislation came into existence. However, with introduction of the Consumer Protection Act, 2019 and its subordinate Consumer Protection (E-commerce) Rules, 2020, several crucial areas which were not dealt with by the previous Consumer Protection Act, 1986, have now been duly incorporated in the new enactments. This is an instrumental step towards guaranteeing rights to consumers and thereby bolstering the protection framework in India, provided effective implementation of the laws and procedures that have been established.

³⁴Neelam Chawla, *E-Commerce and Consumer Protection in India: The Emerging Trend*, JOURNAL OF BUSINESS ETHICS, 581, 586-587 (2020).

ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ARBITRATION: A PLETHORA OF TECHNOLOGY?

-Avantika Singh¹

ABSTRACT

Globalization isn't a new episode watched and lived by us. We have been born and brought up in this ever-growing dynamic living environment. To say that technology is just another limb of globalization cannot be very far from today's reality. Use of technology and artificial intelligence (hereinafter referred as "AI") can be dotted back to the era of embracing the internet with respect to legal field.²

Arguably, the use of AI in arbitration has been more significant as compared to in litigation due to a very simple reason i.e., litigation has witnessed more nightmares in the sense of procurement and implementation.³ Like all that glitters isn't gold, utilization of information technology for the purpose of arbitral processes has been stuck in the infancy stage.⁴ The legal world, globally, has been walking on egg shells when it comes to using information technology with respect to arbitration as it not only contravenes the procedural safeguards but also has the capacity to compromise the quality of justice at a great length.⁵

The International Arbitration does not shy away from this debate. Furthermore, there has been a division in opinions at the international level. Some consider the technology and AI to be the cornerstone is the Legal History, the handing over to the next generation or turning of the page, whichever way you want to say it. Others believe that, with the technology moving at the speed of the light, the loopholes and exploitation of the Judicial System is too easy.

¹ The author is in their 4th year at NMIMS, Navi Mumbai.

² *Arsic, Jasna. "International Commercial Arbitration on the Internet – Has the Future Come Too Early?", Vol. 14, Issue 3, Journal of International Arbitration, Kluwer Law International BV, Sept. 1997, pp. 209–21. Crossref, doi:10.54648/joia1997026.*

³ L. Tyrone Hol, *Whither Arbitration – What Can be Done to Improve Arbitration and Keep out Litigation's Ill Effects*, Volume 7, DePaul Business & Commercial Law Journal (2008) Available at: <https://via.library.depaul.edu/cgi/viewcontent.cgi?article=1120&context=bclj>

⁴ Kaufmann, G., *The Use of Information Technology in Arbitration*. (2005) Available at: <http://lk-k.com/wp-content/uploads/The-Use-of-Information-Technology-in-Arbitration.pdf>

⁵ *Id.*

In this article, I will elucidate:

1. The worldwide debate on use of AI as Arbitrators in International Arbitrations;
2. Whether the plethora of technology is indeed a step back for the Judicial System worldwide?
3. Whether the right to use of technology should compromise the quality of justice

I. INTRODUCTION

In the age of the 21st century discussing AI as arbitrators and legal practitioners, is not an out of the box question. We are governed by technology, fascinated and facilitated by it. Hence, technology coming for our jobs is just another reroute of the capitalist marketers. In every inch of turn of this white-collared world, technology has been augmented into our lives.

International arbitration often necessitates a grasp of domestic as well as international legal system simultaneously. International Arbitration is a spectrum of law which is document intensive, in a sense, that arbitrators and counsels are required to facilitate countless hours for legal research and document reviewing. This is where the use of AI proves to be beneficial as it cuts down time exponentially.⁶

Eminent personalities of the legal playfield have advocated the use of AI in international arbitration to suffice the pressure of mounting case load and documentation. This is due to the escalating demand for speedy and efficient settlement of disputes.⁷ AI not only offers substantive potential to manage and diagnose cases & inefficiencies of arbitral procedurals but also has the ability to augment cognitive functions of human brain and perform it without any hint of delay.⁸ Use of technology is an element of globalization that signifies economic growth, especially in the developing nations. AI takes this economic development a limb further.

As the title of the research exemplify, this paper aims to narrow down the answers for some highly debated and controversial questions with respect to International Arbitration and AI

⁶Thomas R. Snider, *Artificial Intelligence and International Arbitration: Going Beyond Email*, AL Tamini & Co., Available at: <https://www.tamimi.com/law-update-articles/artificial-intelligence-and-international-arbitration-going-beyond-e-mail/>

⁷ Winston Maxwell, Laurent Gouiffès, and Gauthier Vannieuwenhuyse, *The future of arbitration: New technologies are making a big impact and AI robots may take on human roles*, Hogan Lovells, Available at: <https://www.hoganlovells.com/en/publications/the-future-of-arbitration-ai-robots-may-take-on-human-roles>

⁸ Megan Turchi, *The future of International Arbitration may not be AI*, Thinkset, Available at: <https://www.thinksetmag.com/issue-7/ai-may-not-be-the-future-of-international-arbitration>

II. IS AI COMPETENT ENOUGH TO TAKE OVER THE WORLD RENOWNED AND HIGHLY EXPERIENCED ARBITRATORS?

Under Section 11 of the Arbitration and Conciliation Act, 1996, any person, of sound mind, can become an arbitrator. This person can be someone with a legal background like judge, advocate or someone who does not belong to law entirely like chartered accountant, maritime expert, engineer or a businessman.

In India, Arbitration has been gaining momentum since the past decade, especially in commercial litigation. Arbitrators like retired CJIs have passed awards in various arbitral matters. In such a situation, the competency of AI will obviously be put under a skeptic lenses. AI being competent enough to take over arbitrators is not only going to put many out of their profession but also undermine the authority of a highly reputed jurist and, or, legal professional.

HENCE, the question substitution of arbitrators with AI is a very crucial first pillar of this fiasco. There are 3 essentials that play a grave role in determining the above question:

- a. Language and interpretation of law
- b. Programming and database of AI
- c. Precedents set by International Courts.

A. Language and interpretation of the law:

AI has already shattered the glass wall into the legal field. Language of a statute and its interpretation plays a massive role in determination of justice and arbitral award. International Arbitration has experienced its fair share of ambiguity when it comes to language of law pertaining to arbitrators being humans specifically.

“*Convention on Recognition and Enforcement of Arbitral Awards*”⁹ has been silent in its definition of “*arbitrators*”.¹⁰ As the Convention was signed and ratified before the intervention of Web 2.0 and AI, “*arbitrators*” are assumed and hence interpreted as human.

⁹ United Nations Commission on International Trade Law, http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention_status.html

¹⁰ Convention on Recognition and Enforcement of Arbitral Awards 1958, Article I (2) and Article V (1) (b) (USA).

In domestic laws of many nations, a natural person is preferred over a legal person as an arbitrator.¹¹ For that matter, Dutch Code of Civil Procedure under Article 1023 explicitly mentions the appointment of a natural person as an arbitrator.¹² The same has been observed under Article 1450 of Code of Civil Procedure of France¹³ and under and Portuguese Voluntary Arbitration Law.¹⁴

When it comes to international arbitration and laws with respect to it, the language of the law does not affirm or deny the appoint of natural persons as arbitrators, expressly, though the interpretation and procedure of appointment is such that it can only be fulfilled by the former. A small example to explain this can be observed in the laws of Vietnam¹⁵, Indonesia¹⁶, North Korea¹⁷ and China¹⁸. These countries have provided “*year and certain level of experience*” as an essential condition to be appointed as an arbitrator.

The gravest drawback in strengthening the international arbitration laws is that it hasn't defined *natural person* and hence the existence of the former is based on assumption. In such a case, appointment of an AI as an arbitrator is arguably easy.¹⁹ Though, if the parties to the dispute have consented to appoint an AI as an arbitrator, it cannot be superseded by any law on the mere basis of language and interpretation.

B. Programming and Database of AI:

There have been instances and examples where software has been used in law on a daily basis. Intervention of AI can seem like a huge step but in reality it is a mixture of many small steps that have now taken an evolutionary turn.

¹¹Hope, J. (2019) *Can a Robot Be an Arbitrator?* STOCKHOLM ARBITRATION YEARBOOK 103, 111

¹² Dutch Civil Law, <http://www.dutchcivillaw.com/civilprocedureleg.htm>

¹³French Code Of Civil Procedure in English (2019)

¹⁴ Portuguese Arbitration Association, The Portuguese Voluntary Arbitration Law, <https://arbitragem.pt/en/apa/projects-legislation>.

¹⁵The Law on Commercial Arbitration <https://eira.energycharter.org/component/attachments/attachments.html?id=5527&task=download>

¹⁶ Arbitration and Alternative Dispute Resolution Act [http://www.flevin.com/id/lgsso/translations/Laws/Law%20No.%2030%20of%201999%20on%20Arbitration%20and%20Alternative%20Dispute%20Resolution%20\(no%20elucidation\).pdf](http://www.flevin.com/id/lgsso/translations/Laws/Law%20No.%2030%20of%201999%20on%20Arbitration%20and%20Alternative%20Dispute%20Resolution%20(no%20elucidation).pdf)

¹⁷ The Law on External Economic Arbitration <https://www.international-arbitration-attorney.com/wp-content/uploads/2013/07/North-Korea-Arbitration-Law.pdf>

¹⁸Zhonghua Renmin Gongheguozhongcaifa <http://www.cmac.org.cn/wp-content/uploads/2018/08/Arbitration-Law-of-the-Peoples-Republic-of-China-2017-Amendment.pdf>

¹⁹Moses, L.B., *Recurring Dilemmas: The Law's Race to Keep up with Technological Change*. U. ILL. J.L. TECH. & POL'Y 239, 250-54, (2007)

SmartSettle is one such software. It is a small cause claim software which generates numerical issue with respect to two-party negotiation and payment plan.²⁰ Then comes *AdjustWinner*. This software ensures division and distribution of goods amongst the disputing parties in a fair and just manner.²¹ The paradigm shift was brought by *Mondria*- the online dispute resolution software of e-bay.²² Mondria settles customer disputes regarding rules and regulation of e-bay virtually.

Software such as mentioned above have been proved effective as a case management instrument. The outcome of assistance of AI and software has been witnessed by the world in the form of *ROSS*. IBM's data processing AI, ROSS, is world's first AI attorney that has already assisted approximately 50 human lawyers in cases with respect to bankruptcy.

C. Precedents of International Courts

a. U.S. Supreme Court

A study by Katz in 2017 prepared a model which aimed to predict and analyze the legal decisions of the US Supreme Court's decisions between 1816 and 2015, which comprised of 28,009 cases. This work stands out because it employs a significant amount of training data and powerful machine learning technologies, in contrast to other studies that used far less data.²³

A model was assembled by selecting several sets of input data, such as case history and content²⁴, the Circuit Court of Appeals from which the appeal originated²⁵, the time of oral argument and the chronology of the case itself²⁶, and the voting patterns of the individual Justices involved.

An initial subset of the dataset was used for training, and then the algorithm was applied to the rest of the dataset to answer two questions: 2) How each individual Justice voted on the question of whether or not to uphold the Court's decision. When compared to similar models, this one performed exceptionally well, correctly predicting 70.2% of Supreme Court rulings and 71.9% of Justices' votes. A number of issues with the U.S. Supreme Court study remain

²⁰ Smartsettle, <https://www.smartsettle.com/about-us/vision-speech/>

²¹ Adjusted Winner NYU EDU, <http://www.nyu.edu/projects/adjustedwinner/>.

²² Mondria, <http://mondria.com/>

²³ Sivaranjani et al.,

²⁴ Katz et al.,

²⁵ *Id.*

²⁶ *Id.*

unanswered, and it is unclear how widely this research may be applied to arbitration despite its obvious effectiveness. As Scherer pointed out in a recent piece on the subject, first, it is unclear if the model can be effectively adapted to lower court rulings given that these courts are tasked with resolving disputes rather than serving as an appeal body. This is due to the fact that few variables in the training data really pertain to the substance of the disagreement, as opposed to, say, the background or timeline of the case or the behaviour of the Justices. In addition, the research was conducted only on instances when the Supreme Court of the United States has reviewed lower court rulings. Therefore, it does not use instances in which the Court has original jurisdiction as part of its training data.

This is so because Court's judgement might lead to a nuanced conclusion that does not reduce to a simple yes/no answer as to whether the lower court's decision is overturned or upheld.

However, unlike appellate courts, arbitral tribunals are charged with settling disputes rather than reviewing the judgement of a higher court or panel. In addition, the issues of fact and law at stake in international arbitration conflicts can be extensive and difficult to reduce to a simple yes/no framework. As a result, whether or not an AI model can predict a case conclusion when the data are very complicated and not readily translated to a binary categorization is still up in the air. Second, the model did not just learn from variables connected to the internal substance of the cases and the real court documents, but also from features linked to the political leanings of the Justices.

In the United States, judicial nominations are sometimes very politicised, and judges' party leanings can influence their rulings. In other parts of the world, however, the selection of judges is not often based on politics. The study's overarching objective to develop a generic model looks to be unrealistic due to this limitation. As for arbitration, one may contend that the political leanings of arbitrators matter more in the case of investment arbitration. Arbitration in international business transactions, on the other hand, is more fact-based.

For this reason, the primary aspects of the mentioned research model, which have to do with the political leanings of judges, may not be as relevant in international arbitration.

b. European Court of Human Rights

In a highly regarded study, the researchers used precedent cases to train machine learning algorithms on three articles of the European Convention on Human Rights- prohibition on torture under Article 3, protection of the right to a fair trial under Article 6, and protection of the right to respect for private and family life under Article 8.

The most striking aspect of this research is that, in contrast to a study of the United States Supreme Court, neither contextual or temporal factors or the political leanings of the Justices were factored into the model. The researchers noted that the language taken from the decisions' procedural, factual, and legal portions (but not the operative provisions), where the Court announces its conclusion, was utilised for the study. After training, the model made predictions utilising the entire text that were accurate 79% of the time. Researchers also found that getting an accuracy of 73% by focusing exclusively on the details of the events was possible.

This study has a high success rate; however, it has some major flaws. To begin, the researchers only had access to the verdicts themselves and no other paperwork associated with the cases. In this case, the prediction tasks relied solely on the language of the published rulings, rather than the petitions or briefs filed with the Court.²⁷ Without access to the component of the decision that provides the court's legal reasoning, the parties have no way of knowing what the judge will rule on in advance of the trial.

So, the model transformed one conclusion into another, and one judgement into still another. A judgment's applications, briefs, and other key elements are not reassembled to create a new whole. This leads to critical concerns regarding the model's usefulness for preemptively predicting the results of decisions. Secondly, the study's evaluations were predetermined to support the conclusion. Because of this, it is difficult to forecast outcomes in advance based on the judgement texts alone. Furthermore, the term "legal reasoning" pretty much says it all. Information gleaned from the law section often includes the judges' justifications for finding a violation or finding no violation, and on rare occasions, the verdict itself. For example, take the following text drawn from the case of *Velcheva v. Bulgaria*, one of the examples listed in the study, as a result, "Article 61 of the Convention has been violated".

²⁷Aletras et al.

It is unclear from the report if researchers deliberately removed such phrases from the analysis, although it appears that they did not.²⁸ No lawyer is needed to determine whether or if this remark is a breach of Article 6 of the European Convention on Human Rights, which guarantees the right to a fair trial.²⁹ When all the arguments and conversations are written into the verdict itself, it will become clear whether or not there was a breach. Therefore, it is dubious to use such potentially biased data for ex post facto prediction.

Lastly, the model relied on the Court's description of the facts rather than the parties' own descriptions of the facts, which is problematic for ex-ante result prediction. Researchers acknowledge this caveat by noting that the ECtHR's fact compositions might be altered to get a desired result, but they still draw the conclusion that the case's facts are the most predictive factor.

This perspective is also endorsed by Morison and Harkens, who said the facts are not in question at this level because the ECtHR is as an appeals court, and therefore make no issue to this.

Meanwhile, Pasquale and Cashwell joke that the study's approach is similar to "predicting" the nature of a cuisine based on its nutritional profile. While it might be claimed that the ECtHR is bound by the findings of fact made in the domestic courts.³⁰

For the time being, at least, a model can only use data from previously solved problems to anticipate the results of new decisions.

The actual prizes and their internal content are thus still significant for predictive purposes until a "complete" model is constructed and a database for it is produced. In contrast, the researchers found that the content parts of the ECHR judgements were clearly divided, facilitating uniformity and therefore enabling text-based analysis.

Although international arbitral judgments are more thorough than domestic awards, it is not always obvious what constitutes a reasoned award or how to prepare one in the context of international commercial arbitration. If an arbitral award's textual content were to form the basis of a model, there would be difficulties in separating factual results from legal conclusions. The technique adopted by civil law and common law courts when making

²⁸ Aletras et al., supra note 26.

²⁹ Velcheva v. Bulgaria, App. No. 35355/08, para. 40.

³⁰ Garcia Ruiz v. Spain, 1999-I EUR. CT. H.R. 87 (1999)

awards is different, which is another connected difficulty. The former uses a "instances-to-principles" line of thinking, whereas the later uses "principles-to-instances"

Even though a judgement is clearly split into various subject portions, the nature of the material may nevertheless vary depending on whether the arbitrator was educated in a civil or common law country. Finally, the ECHR study's data originated from a court of last resort, or apex court, just like the U.S. Supreme Court study's data did. However, unlike judicial review, international commercial arbitration is fact-based and seeks to resolve conflicts on their merits rather than relying on precedent. When a case cannot be simply reduced to a binary categorization (violation/no violation, affirm/reverse, etc.), it raises the question of whether an AI model can accurately anticipate the conclusion.

III. ISSUES PERTAINING TO TAKE OVER BY AI TAKES OVER

1. Amendments in Major Sets of International Arbitration Rules

The International Chamber of Commerce (ICC), American Arbitration Association (AAA) and London Court of International Arbitration (LCIA), have their own set of international arbitration rules. Specialized entities like as WIPO are increasingly joining them in developing sector-specific arbitration systems. Due to these extensive alterations, international business arbitration is anticipated to become more widely utilised. It is crucial to evaluate the various arbitral regimes and how the new regimes will affect the uniformity and predictability of resolution of commercial international disputes.³¹

The rules regulating administered arbitrations are changing the most, as these are the arbitrations that will be managed or supervised by an institution to varying degrees. In contrast, ad hoc arbitration is conducted by the parties.

The parties to ad hoc arbitration may opt for a preexisting set of rules, such as the UNCITRAL Model Rules. Institutional arbitration rules, such as those of the ICC, the AAA, and the LCIA, can have an impact beyond the arbitrations they directly oversee since ad hoc arbitrations might adopt them as their own. Moreover, they are invaluable resources for both arbitral institutions and private parties as they craft their own arbitration terms in contracts.

³¹ Gwyn, A.H. and Benjamin O. Tayloe, Jr. *Comparison of the Major International Arbitration Rules*. 19 CONSTRUCTION LAW 23, (1999)

The modifications that have been made to ICC, AAA, and LCIA are minor practical adjustments to operating regulations. When placed in perspective, however, these shifts reveal the consequences of the worldwide expansion of trade. International arbitration legislation is being adopted by several nations in favour of older, more general laws that were only drafted to cover domestic disputes."³²

2. Choice of Law Clause

The first contentious issue, which has long plagued American law and practice, is the question of how to determine the applicable law in international arbitration agreements. A choice of law provision is common in arbitration agreements involving foreign parties.

Recent trends in international arbitration practice highlight the need to include a choice of law clause to clearly identify the applicable law for the entirety of the parties' contract. However, court intervention may be required to resolve the pre-arbitration issue where the parties' interpretation of this arbitration agreement differs. For the most part, a court will defer to the parties' choice of law to regulate a contract. Commercial arbitration law continues to face challenges and uncertainty in the area of proper execution of parties' stated choice of law agreements in U.S. courts.

US Supreme Court devised a method in "*Mastrobuono v. Shearson Lehman Hutton*"³³ that maintains the parties' autonomy in deciding whether to integrate particular rules of arbitration via the stated choice of law provision. The standard applied by the court is whether or not this option can be projected impartially from the text of the agreement. The correct application of a choice of law provision can, hence, be determined by using these objective criteria. Pre-*Mastrobuono* precedent held that, while the law of the contracting parties' domiciled nation would govern issues of arbitrability and validity of the arbitration agreement, the national law (i.e., the *lex fori*) would govern issues of content.

As a result, allegations of non-arbitrability regarding public policy were rejected under U.S. law, as contained in the Federal Arbitration Act (FAA).³⁴ Let's say, for the sake of argument, that a certain contract has both, arbitration clause and a choice of law clause, that are both

³² Christopher R. Drahozal *Commercial Norms, Commercial Codes, and International Commercial Arbitration*, 33 VAND. J. TRANSNAT'L. 79, 120, (2000).

³³ *Mastrobuono v. Shearson Lehman Hutton* 514 U.S. 52 (1995).

³⁴ Federal Arbitration Act, 9 U.S.C. §§ 1-16, 201-10,301-07 (2001) (USA).

extremely broad in scope. During the course of a dispute, the argument may develop that some topics at stake are not amenable to arbitration under the selected legislation. The precedent, which relied on the separability concept, required the arbitration clause as a standalone agreement. This arbitration provision shall be deemed to be obligatory and hence enforceable with the Federal Arbitration Act. The arbitrator, not a judge, would hear the parties' arguments about whether or not a certain issue is subject to arbitration.

With its judgement in "*Volt Information Sciences, Inc. v. Board of Trustees in 1989*"³⁵, however, the Supreme Court of the United States refocused its attention on the arbitration agreement's voluntary nature. Instead of the separability theory being the focus of analysis, the idea of party autonomy emerged as the most important concept. The autonomy of the parties allowed them to agree on a body of legislation that would preclude the arbitration of some disputes on public policy grounds. If that legislation was used as the basis for the arbitration clause's choice of law, it would be more likely that a court would find the issue to be non-arbitrable and thereby prevent it from going to arbitration. Both the courts and the academic community were harsh in their assessment of Volt.

This seemed to downplay the importance of government policy encouraging arbitration of conflicts and posed a danger to the efficacy and credibility of generally acknowledged dispute resolution methods in cross-border business dealings.

To mitigate Volt's impact, some judges have argued that a clear indication that an ousting of federal law was intended should be included in the choice of law clause. The disputes with respect to claims being punitive damages can be taken to arbitration. For instance, New York law appears to permit punitive damages in court lawsuits but not in arbitration verdicts. Imagine a contract that specifies New York law and provides for mandatory arbitration. Punitive damages: may they be given by an arbitrator? Some courts have given that answer based on Volt, reasoning that New York law must be followed. Still others argued that federal law should be applicable as the choice of law clause only talks about substantive law of contract while excluding its arbitrability. United States Supreme Court revisited the question in *Mastrobuono*, aiming to find common ground linking the theory of party autonomy and the separability doctrine. While the intentions of the contracting parties are still relevant, the arbitration provision must be analysed independently according to the

³⁵ *Volt Information Sciences, Inc. v. Board of Trustees* 489 U.S. 468 (1989).

separability concept. In the absence of a mutual agreement by the parties to waive punitive damages, the matter must be sent to arbitration.

IV. AUTHOR'S PERSPECTIVE

AI Arbitrators sounds like an intermingling between Metaverse and ChatGPT. As much as we all want them to assist us and ease our lives, we are well aware of the shortfalls and authenticity.

After the research analysis above, few pointers that can be narrowed down are:

1. As far as the language of prevalent law is concerned, AI can be appointed as an Arbitrator. This is possible due to three very simple yet challenging facts:
 - a. Firstly, the definition of “arbitrators” as per various legal literature does not limit itself. In simpler terms, the definition has a very broad sense of interpretation, which entails and leads to inclusion rather than being exclusive.
 - b. Secondly, the definition of arbitration contains “natural person”. Now as a premise, the definition of natural person should have been mentioned in order to determine the walls and boundaries of the words. In the present case, as there exists no definition of natural person internationally, in the sense of arbitration, the inclusion of AI as an arbitrator is fairly easy, which in turn leads to exploitation of the resources currently prevalent in society. In order to limit unnecessary exploitation of legal statute and literature, the premise of a word has to be interpreted in such a way that it does not lead to exploitation of law at the hands of a third party. In the present case, such situation is not possible for a simple reason that there are no defining boundaries.
 - c. Lastly, in the due course of interpretation of language of law, the programming language used and database present also plays a crucial role, in a sense that it provides for a set of precedents in an unchartered territory with reference to AI and law. The same goes for precedents present in law in form of judgements, which act as documentation of resources in matters which are highly debatable yet not properly documented.
2. International rules pertaining to arbitration have suffered gravely due to the ambiguity in respect of choice of law. This issue is only going to intensify when AI comes into play.
3. AI can act as arbitrator provided none of the party contest it. But should AI act as arbitrator is the question of the hour. Throughout various literature and the work presented herein, it is

clear as glass that AI will be a beneficial and paradigm shift in the course of arbitration but the same literature and work also foresees the disruption in law brought by artificial intelligence.

- a. Law, especially arbitration, is a field which required emotional quotient to negotiate, arbitrate and understand the legal semantics of a situation. Without emotional intelligence, advocates and lawyers are battery operated robots with profit earning as the only goal. Such is the situation if arbitrators are replaced. Emotional intelligence, that is EQ, of an advocate is challenged and tested at every stage of proceedings and due to which, the no proceeding is black and white.
- b. Recently, a Washington Times post declared that constant running and usage of data for ChatGPT has resulted in a money losing model. Such thing will repeat itself on a constant as using an AI as arbitrator is not going to be a cheap or easy investment. This in return will hamper the middle-class structure gravely because with rise in cost of production and maintenance of an AI, the cost to access such facilities will also be influenced creating an unprecedented, invisible yet highly predictable discrimination amongst member of the society, challenging their right to equality. Law as a field has to sustain each individual in society. This will be completely altered.

V. CONCLUSION

What AI in arbitration brings to the table is increase in participant's access to information about the probability of claims succeeding, the best strategies employed in arbitral processes to increase success rates, unbiased arbitral panel selection procedure, and other significant issues at a lower cost. Despite the difficulties discussed in the preceding section. As a result, the following are some potential solutions to the problems that AI faces when used in arbitration.

Both the arbitrators and the attorneys in the arbitration process should always keep in mind that keeping client confidences secure is an integral aspect of providing professional representation. One strategy to address the issue of bias in AI algorithms is to increase attention paid to the data used to train machine learning systems, which can help prevent the development of biased AI systems. In addition, nonbiased results require diversity in the machine learning community to identify and correct instances of bias in AI.

Confidentiality in arbitration and ever-evolving nature of AI fall short in generating accurate outcomes backed by sufficient information. Even-though it hasn't been completely implemented yet, AI can prove to be of good use in the domain of arbitration, where it has already shown its mettle in the form of superior performance on jobs requiring analytical processing.

The arbitration sector is one area where AI has opened the floodgates to change. The potential benefits of AI greatly outweigh its drawbacks. The issue of where to draw the line of involvement is a persistent one. The ideals of arbitration would be undermined if AI were given entire control of the arbitration process. However, if AI is entirely debunked, cases will continue to be stalled because the courts will be made to look like they are too busy. Therefore, a middle ground must be taken in order to enjoy the benefits of technology while yet upholding the norms of arbitration.

Arbitrators can employ AI to help them in their work. Using Weak AI to streamline processes may help get disagreements settled more quickly. In the context of arbitration, AI might manage the admission of claims, collecting of arguments, thorough investigation into history of conflicts, and potential arbitration verdict based on precedents and accessible data. Conversely, human mediators can handle complex communication issues. AI can help in choosing qualified arbitrators.

New York Dispute Resolution Journal states that “*heavy amounts of material may be summarised by simple classification and grouping methods*”, by arbitration and hence making it a better dispute resolution process as compared to litigation in terms of cost and time. With the aid of AI technologies, the award may be drafted with ease by simply inserting important snippets of facts, common and contested viewpoints of the parties, and procedural history. An approach somewhere in the centre, one that embraces diversity and inclusion, may be very useful for the legal profession. Arbitration might benefit from the use of AI, but it should not be permitted to handle all cases on its own.

CENTRAL BANK DIGITAL CURRENCY: RENOVATING THE INDIAN FINANCIAL SECTOR

-Swarna Yati¹

I. INTRODUCTION

With the exponential growth of cryptocurrencies and stablecoins, the central banks of various countries decided to launch their own virtual currencies. A CBDC would be the most secure digital asset accessible to the general public, with no associated credit or liquidity risk, as it is a liability of the Central Banks.² Such an attempt, with the aim of revolutionising the Indian economy, and after the whopping success of the Unified Payments Interface (UPI), the Reserve Bank of India, in October 2022, launched the proposal for Central Bank Digital Currency (CBDC).

Currently, 95% of the global economy is trying to incorporate digital currencies into their economy. About 11 countries have fully launched digital currencies, and about 20 are in the experimental phase, including India.³ India has entered its pilot phase with the launch of CBDC for a closed group.

The CBDC is also in the ore-launching phase in the United States as the Federal Reserve Board tries to weigh the pros and cons of digital currency and build an infrastructure for its introduction in the U.S. markets.⁴

CBDC can widely be classified into two categories: Retail CBDC and Wholesale CBDC. This distinction is made based on the sector in which the two are used.⁵ Retail CBCDs are intended for usage by consumers, homes, and businesses, whereas financial firms are designed to employ wholesale CBCDs and would be available to select financial institutions.

¹ This paper is authored by Swarna Yati of 3rd year studying in Dr. Ram Manohar Lohiya National Law University, Lucknow.

² Stanley, Andrew. (2022) *The Ascent of CBDCs*, IMF. Available at: <https://www.imf.org/en/Publications/fandd/issues/2022/09/Picture-this-The-ascent-of-CBDCs>.

³ *Central Bank Digital Currency tracker* (2022) Atlantic Council. Available at: <https://www.atlanticcouncil.org/cbdctracker/>.

⁴ *Central Bank Digital Currency (CBDC)* (2022) Federal Reserve Board - Central Bank Digital Currency (CBDC). Available at: <https://www.federalreserve.gov/central-bank-digital-currency.htm>.

⁵ *Central Bank Digital Currency (CBDC) pilot launched by RBI in the retail segment has components based on Blockchain technology* (2022) Press Information Bureau. Available at: <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883>.

II. GLOBAL SCENARIO

The first digital currency launched in any significant economy, RBM, was launched in China.⁶ China began testing the Digital Yuan-Digital Renminbi in May 2020.⁷ An analysis of the CBDC rolled out in China indicates that digital currencies are the way to the future and have exponential scope for improving the country's economy.

Digital yuan transactions surpassed the \$14 billion (100 billion yuan) mark on October 10, in contrast to the \$12 billion (87.6 billion yuan) recorded by the People's Bank of China at the end of 2021.⁸ In its recent attempt to boost the adoption of the digital yuan, the Chinese CBDC wallet has decided to introduce the traditional red envelopes. As a consequence of the rise in popularity of digital payments, well-known local services like WeChat Pay and Alipaynow provide virtual red envelopes.

Fabio Panetta, a member of the European Central Bank (ECB) executive board, has been a prominent proponent of central bank digital currency (CBDC) and a critic of cryptocurrencies.⁹ He is attempting to promote digital money, which will preserve the public's confidence as they transition to risky cryptocurrencies out of a sense of not wanting to miss out.

The Kazakhstan government is also working towards incorporating digital currencies into its economy. According to the central bank of Kazakhstan, CBDC should be made accessible as early as 2023, with a progressive increase of capabilities and entry into commercial operation by the end of 2025.¹⁰ President Kassym-Jomart Tokayev also applauded digital currency for being secure and reliant and asserted that it would be given recognition.

⁶ Buchholz, K. (2021) *China becomes the first major economy to issue digital currency*, *The Wire*. Available at: <https://thewire.in/world/china-becomes-first-major-economy-to-issue-digital-currency>.

⁷ Bansal, R. (2021) *China's Digital Yuan: An Alternative to the Dollar-Dominated Financial System*, *Carnegie Endowment For International Peace*. Available at: https://carnegieendowment.org/files/202108-Bansal_Singh_-_Chinas_Digital_Yuan.pdf.

⁸ Srinivasan, K. (2022) Opening remarks at peer-learning series on Digital Money/Technology: Central Bank Digital Currency and the case of China, IMF. Available at: <https://www.imf.org/en/News/Articles/2022/07/07/sp070722-central-bank-digital-currency-and-the-case-of-china>.

⁹ Andersen, D. (2023) *ECB official urges CBDC development for the good of cryptocurrency and consumers*, *Cointelegraph*. Available at: <https://cointelegraph.com/news/ecb-official-urges-cbdc-development-for-the-good-of-cryptocurrency-and-consumers>.

¹⁰ Popowicz, J.E. (2022) *Kazakhstan explores crypto co-existence in Binance CBDC trials*, *Central Banking*. Available at: <https://www.centralbanking.com/fintech/cbdc/7954054/kazakhstan-explores-crypto-co-existence-in-binance-cbdc-trials>.

In order to grow CBDC over the next three years, the Kazakhstani government is concentrating on technological advancements, infrastructural preparation, creating an operational model, and establishing a regulatory framework.

III. INDIAN SCENARIO

Currently, CBDC is still in its research phase in India and is being tested in four cities through four banks. In the initial phase, the Central Bank will issue CBDC to these banks.

This step will boost the Indian market by expanding the digitalisation of currency and internationalisation. The amalgamation Of UPI and CBDC will boost cross-border transactions and, thus, the business. Other common reasons for introducing CBDC include fostering competition and resilience in the domestic payments market, which may need incentives to offer cheaper and better access to cash, improving payment efficiency and lowering transaction costs, developing programmable currency and enhancing money flow transparency, and facilitating the quick and straightforward flow of cash and lower transactional cost.¹¹

Due to the on-chain settlement capabilities built into digital currencies, blockchain experts think a digital rupee running on UPI rails would guarantee 0% payment transaction failure. In places with patchy internet access, it will be a game-changer.

Until now, the Reserve Bank has recognised nine prominent banks to be a part of this pilot project. It includes the State Bank of India, Bank of Baroda, Union Bank of India, HDFC Bank, ICICI Bank, Kotak Mahindra Bank, Yes Bank, IDFC First Bank and HSBC.

The digital rupee would be a digital token for legal tender. It would be distributed in the same denominations that coins and paper currency are now issued. It can be sent or received in digital wallets and can be stored on mobile phones. Unlike UPI, which is linked to a bank account, it is independent of the account, and no money is deducted from the bank account to

¹¹ *Central Bank Digital Currency (CBDC) pilot launched by RBI in the retail segment has components based on Blockchain technology (2022) Press Information Bureau. Available at: <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883>.*

complete the transaction. The transaction can be from person to person(P2P) or person to merchant (P2M).¹²

The development of CBDC will boost the current government's Digital India mission, enabling more cashless transactions. It must be realised that the adoption of digital currency would be possible only when there is a high percentage of digital perforation¹³ and digital know-how in the country.

IV. CBDC vs CRYPTOCURRENCY

The RBI forbade financial institutions from engaging with cryptocurrencies in 2018, which caused various sites to shut down. The judgement was overturned, nevertheless, by a Supreme Court ruling in March 2020 that permits cryptocurrency-related businesses in India to resume. With the decision to launch its own digital currency, many would believe that RBI has taken a 180-degree turn in its stance, but it is not. This digital currency has a few similarities with cryptocurrencies; it differs greatly from it.

Similar to cryptocurrencies or bitcoins, the digital rupee is also based on blockchain technology. Although, unlike bitcoins, cryptocurrencies and stablecoins, which run on distributed ledger technology, are centrally monitored by central governments. Cryptocurrency is based on the principle of decentralisation, whereas the nations' central banks back CBDC and hence is more secure and promising.

Another distinction is that CBDCs utilise a private Blockchain network with prior authorisation, whereas cryptocurrencies use an open network that requires no permission.

Additionally, users remain anonymous when they transact on the web utilising bitcoins. CBDCs, on the other hand, will be connected to a person's bank account, which contains their personal information. In contrast to other virtual currencies, CBDC is not volatile, and its value equals the value of physical currencies.

¹² *Central Bank Digital Currency (CBDC) (2022) Federal Reserve Board - Central Bank Digital Currency (CBDC)*. Available at: <https://www.federalreserve.gov/central-bank-digital-currency.htm>.

¹³ Srinivasan, K. (2022) *Opening remarks at peer-learning series on Digital Money/Technology: Central Bank Digital Currency and the case of China, IMF*. Available at: <https://www.imf.org/en/News/Articles/2022/07/07/sp070722-central-bank-digital-currency-and-the-case-of-china>.

Cryptocurrencies and bitcoins are also seen as investment portfolios, whereas CBDC is a standard nationalised legal tender, which would not accrue any interest or profit over time. In the current scenario, where cryptocurrencies are being used for terror funding, money laundering and tax evasion, CBDC will create a more transparent cyberspace where these transactions can be prevented.

V. ADVANTAGES

The Reserve Bank of India plans to launch digital currency after much deliberation and discussion. The benefits posed by such digital currency include Real-time money transfer, easy currency tracking, difficulty in tax evasion, and reduction of money-related crimes such as money laundering. This would also help to bridge the gap between bank accounts and mobile phones, which still needs to be solved.

- Money transfers and payments may be made in real time from the payer to the payee without the need for intermediaries like banks.
- Simple currency tracking: By implementing CBDC, a country's central bank will be able to keep track of the precise position of every unit of money.
- Income Tax: It will be tough to evade or avoid paying taxes since techniques like offshore banking and unreported employment cannot be used to conceal financial activity from the central bank.
- Criminal activity such as money laundering and funding for terrorism may be quickly identified and put an end to.
- The introduction of CBDC will also reduce the printing, handling and transactional cost of physical currency.

VI. LOOPHOLES

Albeit its potential, CBDC possesses some serious questions which need to be answered before advancing to the next phase. The first question is about the adoption of the currency by the public, which is still largely dependent on the physical currency. Alternatively, extreme circumstances might lead people to collect vast amounts of CBDC, leading to a crisis.

One of the significant concerns, which was also highlighted by the Governor of RBI, Shaktikanta Das, is the cloning of digital rupees, which might lead to virtual inflation.¹⁴ In the post-Covid world, controlling spiralling inflation is one of the biggest challenges all economies face. With the dwindling condition of Commercial banks in India, the greater adoption of CBDC might lead to the further breakdown of commercial banks.¹⁵ This situation can be avoided by limiting the holding amount of CBDC for consumers.

The concept paper indicates that "banks and other service providers" will participate in the two-tier CBDC architecture. Clarifying the definition of service providers is required to determine if existing RBI-regulated firms will be included or whether emerging participants may be included. It will be necessary to consider the ramifications under the Banking Regulation Act of 1949 and the Payment and Settlement Systems Act of 2007, depending on the financial sector intermediaries participating in the CBDC infrastructure.

CBDC is vulnerable to cyber security issues and can become a target for cyber attacks. The implementation of CBDC also poses consumer protection, data privacy, and anti-money laundering complications. With CBDC, the governments can easily monitor the transactions between the parties, but the question is whether this is against the right to privacy.¹⁶ All these questions still need to be answered in the current notification.¹⁷ Proper legislation and

¹⁴ Ghosh, K. (2023) *RBI approaching CBDC with extreme caution due to threat of cloning: RBI, Outlook*. Available at: <https://www.outlookindia.com/business/rbi-approaching-cbdc-with-extreme-caution-due-to-threat-of-cloning-rbi-governor-das--news-251365>.

¹⁵ Pfister, C. (2017) *Monetary policy and digital currencies: Much ado about nothing? Banque De France*. Available at: <https://www.banque-france.fr/sites/default/files/medias/documents/dt-642.pdf>

¹⁶ Justice K. S. Puttaswamy (Retd.) and Anr. v. Union Of India And Ors, AIR 2017 SC 4161.

¹⁷ *Central Bank Digital Currency (CBDC) pilot launched by RBI in the retail segment has components based on Blockchain technology* (2022) *Press Information Bureau*. Available at: <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883>.

watchdog must be established to keep these issues at bay. Since the currency is supposed to run on internet platforms, it is susceptible to hacking and counterfeiting.

VII. LEGAL ANALYSIS

The emergence of Central Bank Digital Currency in India has sparked a flurry of legal analysis surrounding its implementation and potential implications. Legal scholars have delved into the intricacies of how such currency would be regulated, what laws it would adhere to, and how it may impact existing financial systems.

i. Currency vs Digital Currency

One key examination area is whether or not CBDC can be classified as a legal tender under India's current monetary policies. This consideration hinges on the definition of "currency" under Indian law¹⁸, which may require amendments to accommodate digital currencies within its purview. Relevantly, the Reserve Bank of India Act, 1934 (RBI Act) was modified by the Finance Act, 2022, expanding the definition of "banknote" to include notes produced in digital form. In conjunction with Section 22 of the RBI Act, this change gives RBI the authority to print digital bank notes.

The question of whether the sovereign has unrestricted authority to grant a means of payment legal tender status through legislation or positive law arises in light of the potential legal tender status of CBDC with regard to natural law. It is reasonable to claim that the State may only legitimately provide legal tender status to a form of payment if the great majority of people can easily access it. In other words, it may be permissible to grant legal tender status to a form of payment that the vast majority of people do not accept. However, doing so raises important issues, particularly those of equity and justice.

The designated group of creditors that are required to accept payment in the indicated means of payment must also make efforts to guarantee that payment may be received successfully. This is acknowledged by nations that have granted legal tender status to payment methods that are not currencies.

The legality of CBDCs depends on multiple factors, such as the regulatory framework and existing laws governing currency, payment systems, and banking operations. The Reserve

¹⁸ Publish, N. (2022, November 1). *Legal tender*. iPLEaders. <https://blog.ipleaders.in/all-about-legal-tender/>

Bank of India (RBI) must ensure that the CBDC complies with all financial regulations to prevent potentially illegal activities like money laundering or terrorist financing. Additionally, privacy concerns must be addressed through robust data protection measures to protect consumers' sensitive information from being compromised by hackers or other malicious actors.

ii. The Policy Changes in Implementing Central Bank Digital Currency in India

The legal framework for implementing CBDC in India is still in its infancy. The Reserve Bank of India (RBI) has set up a working group to explore the feasibility of issuing a central bank digital currency, however, concrete plans have yet to be announced. Secondly, the government needs to implement regulations for managing and using CBDC. These regulations will cover issues such as anti-money laundering and countering the financing of terrorism.

Thirdly, the RBI needs to develop a robust technological infrastructure for issuing and managing CBDC. This includes ensuring that CBDC can be easily integrated with existing payment systems and platforms. Fourthly, the RBI needs to consider the economic implications of issuing CBDC. For example, how will CBDC affect inflation? Will it replace cash or complement it? How will it impact interest rates?

Legal clarity on the regulation of intermediaries' companies must be defined if the entry of fresh players is permitted to offer technical or other value-added services. For instance, Nigeria envisions merchants as having the responsibility of offering e-Naira transaction choices. Merchants are described as fully accredited persons and non-individuals (corporates) authorised to conduct business in Nigeria.

It will be necessary to look at the structure of the Know-Your-Customer (KYC) framework and how the Prevention of Money Laundering Act, 2002 (PMLA) is used. Tiered KYC may be taken into consideration because the RBI suggests "managed anonymity" with anonymity for minor transactions and traceability for large-value transactions. Wallets may be allowed to have particular characteristics, such as caps on funds and restrictions, as well as the type of transactions, depending on the degree of KYC. CBDC Intermediaries must be subject to the PMLA Act's rules for "specified transactions".

The RBI needs to engage with all stakeholders – including commercial banks, fintech firms, regulators and consumers – to ensure that everyone is on board with the implementation of CBDC. Only then can India successfully launch its central bank digital currency.

Another critical point that must be considered in framing policies is whether the Indian government wants the currency to be pegged to the rupee or allowed to float freely. This decision will likely have significant monetary policy and financial stability implications.

iii. Data Privacy

The CBDC infrastructure will provide CBDC intermediaries access to a lot of private data. To understand who can collect, handle, and keep data, the objectives for which it will be used, and whether or not the data can be shared with other entities, including RBI and government entities for law enforcement, legal concerns pertaining to privacy and data governance must be considered. Furthermore, it could be necessary to look at the cross-border consequences of exchanging data outside of India. The Information Technology Act of 2000 and the Information Technology (Reasonable security practices and Procedures and sensitive personal data or Information) Rules of 2011 now address these concerns.

The Puttaswamy case¹⁹ and other significant Supreme Court rulings highlighting India's lack of comprehensive data protection legislation make it essential to create robust data governance and privacy standards for safeguarding customer data. Significant problems with the definition of small-value transactions, the limit on such anonymised transactions, the potential for abuse of such anonymised transactions, and the legal safeguards for controlling such transactions come up when "managed anonymity" is implemented.

The Reserve Bank of India (RBI) has previously expressed concerns about cryptocurrencies and their impact on financial stability, prompting us to question whether or not a CBDC would face similar scrutiny. Additionally, questions about data privacy and security must be addressed to ensure that sensitive information remains protected within the proposed framework. A comprehensive legal analysis must consider these factors alongside other issues, such as anti-money laundering regulations and taxation policies related to digital currency transactions.

¹⁹ KS Puttaswamy v. Union of India, AIR 2017 SC 4161.

Furthermore, the legal implications for commercial banks should also be considered as they may face competition from this new form of digital currency issued directly by RBI. As a result, central bank digital currencies can significantly impact monetary policy by giving RBI greater control over the money supply while simultaneously reducing reliance on physical cash transactions. In conclusion, understanding the legal landscape surrounding central bank digital currencies is crucial before their implementation in any country's economic system. This requires extensive consultation with regulators and stakeholders to address any potential challenges that may arise from their use while maintaining transparency throughout this process. Ultimately successful integration into an economy will depend not only on technical feasibility but also on legal compliance within existing frameworks for finance and technology alike.

UNREGULATED EQUITY CROWDFUNDING IN INDIA: A NEED TO FILL THE VACUUM IN THE EXISTING REGULATORY FRAMEWORK

~ Valan A¹

ABSTRACT

Equity crowdfunding is a conducive fin-tech business funding model for emerging start-ups to raise finance in smaller sums from multiple investors through web-based platforms. While the crowdfunding industry has prospected to hike exponentially in the near future, India still lacks a legal framework for regulating equity crowdfunding. Having felt the need for such regulation, SEBI proposed a regulatory framework to regulate crowdfunding through a consultation paper in 2014. Nevertheless, no regulatory measures have been initiated yet by SEBI rather, issued a caution notice to crowdfunding platforms in 2016 and claimed crowdfunding to be unregulated and illegal.

Further, the appropriateness of the SEBI's proposed regulatory framework has been inquired in the light of regulatory theories and the idea of 'crowdfunding'. In specific, the scope of the paper is restricted to critically analyzing SEBI's proposed threshold on investment and investors in crowdfunding, from the perspective of investors and issuer companies.

While the SEBI's proposed regulatory framework adopts a "duck-type (same risk, same rule)" approach for regulating equity crowdfunding on par with the private placement, especially with respect to investment and investor threshold. Therefore, the paper argues that the proposed framework ignores the new functionality of crowdfunding; falls foul under the proportionality principle; and remains impractical and against the core tenets of crowdfunding i.e., to enable investors to participate in investment who otherwise wouldn't have engaged in the conventional capital market. Therefore, it is suggested that SEBI may adopt a "Code (new function, new rule)" approach to regulate crowdfunding with no investor threshold but with an investment threshold in proportion to the investor's risk-bearing capacity, towards balancing investor protection and promotion of entrepreneurship.

Keywords: equity crowdfunding, fin-tech, digital platforms, SEBI

¹ The author is a student in their IV Year at the Tamil Nadu National Law University.

I. INTRODUCTION

SEBI defines crowdfunding as the “*Solicitation of funds (small amount) from multiple investors through a web-based platform or social networking site for a specific project, business venture or social cause.*”² Aftermath of 2008 global financial crisis, the idea of crowdfunding emerged as an alternative to raise capital for entrepreneurial and innovative ventures.³ Globally, the crowdfunding industry is approximately a \$34 billion industry.⁴ It is estimated that crowdfunding would turn a \$ 300 billion industry in 2025.⁵ There are various types of crowdfunding such as Donation-based, reward-based, peer-to-peer lending and equity crowdfunding. Amongst various types of crowdfunding, literature⁶ suggests that, the profit-sharing model of crowdfunding (for instance, by issuing equity shares) would be advantageous for early-stage ventures to fill the resource gap. Equity crowdfunding is a Fintech business funding model which aspires to acquire capital in smaller sums from a varied number of investors through online platforms.⁷

Crowdfunding develops swiftly and so do the associated risks which warrants the regulator’s attention. On one hand, equity crowdfunding would help the entrepreneur to sell the idea to millions of potential investors; need not have intermediary merchant banks; spread risk and boost the economy. On the other hand, the investment in equity crowdfunding is risky as 50% of the start-ups fail during the initial years,⁸ contributors cannot recoup their investments as there is no secondary market,⁹ false disclosure,¹⁰ lack of transparency, the experience of

² *Consultation Paper on Crowdfunding in India*, SECURITIES EXCHANGE BOARD OF INDIA (2014).

³ Paul Belleflamme & et al., *Crowdfunding: Tapping the Right Crowd* 29 (5) JOURNAL OF BUSINESS VENTURE 610 (2011). See also, Aryan Dhingra, *Equity Crowdfunding Conundrum – Rise and Fall of Equity Crowdfunding in India*, THE COMPETITION AND COMMERCIAL LAW REVIEW (January 6, 2020), <https://www.tcclr.com/post/equity-crowdfunding-conundrum-rise-and-fall-of-equity-crowdfunding-in-india>.

⁴ Chet Jainn, *Crowdfunding industry eyes clarity on regulation and legal accountability in Budget 2022*, THE ECONOMIC TIMES (January 29, 2022), <https://economictimes.indiatimes.com/small-biz/sme-sector/crowdfunding-industry-eyes-clarity-on-regulation-and-legal-accountability-in-budget-2022/articleshow/89194162.cms>.

⁵ *Id.*

⁶ Paul, *supra* note 2.

⁷ Nidhi Agarwal, *Taking the ‘Crowd’ Out of Crowdfunding: SEBI Regulations on Equity Crowdfunding*, THE CENTRE FOR BUSINESS AND FINANCIAL LAWS (October 19, 2022), <https://www.cbflnludelhil.in/post/taking-the-crowd-out-of-crowdfunding-sebi-regulations-on-equity-crowdfunding>. See also, Michelle Black & Jordan Tarver, *Equity Crowdfunding: What Is It & How Does It Work?* FORBES ADVISOR (March 31, 2022), <https://www.forbes.com/advisor/business-loans/equity-crowdfunding/>.

⁸ K. Erkki Laitinen, *Prediction of failure of a newly founded firm* 7 (4) JOURNAL OF BUSINESS VENTURING 323 (1992).

⁹ Eleanor Kirby & Shane Worner, *Crowd-funding: An Infant Industry Growing Fast*, Staff Working Paper No. [SWP3/2014], IOSCO RESEARCH DEPARTMENT (2014).

¹⁰ C. Steven Bradford, *Shooting the Messenger: The liability of crowdfunding intermediaries for the fraud of others*, UNIVERSITY OF CINCINNATI LAW REVIEW (2014).

many investors and information asymmetry.¹¹ To address this by bringing equity crowdfunding into the regulatory ambit, SEBI initiated a discussion paper in 2014.¹² Such need for regulation is real and pressing as shares are *primarily a liability*,¹³ where investor protection by ensuring informed consent is a regulator's paramount duty.

Though SEBI has emphasised the significance of equity crowdfunding and the need for regulating it, in 2016, SEBI eventually decided against the idea by issuing a press release which emphasised that equity and other securities could be listed and traded only through recognised stock exchanges.¹⁴ Consequently, the SEBI has shut down several fintech platforms engaged with EC¹⁵ and directed disclaimers for crowdfunding.¹⁶

In this context, the paper attempts to analyse three aspects viz., Current position of unregulated equity crowdfunding in India, possibility of regulating equity crowdfunding within the existing regulatory framework (if any) and appropriateness of the proposals made by SEBI concerning investment and investor threshold.

II. SEBI'S INTENTION TO REGULATE THE EQUITY CROWDFUNDING WITH THE EXISTING REGULATORY FRAMEWORK

As inferred from the introductory chapter, SEBI has taken a firm stand on equity crowdfunding to be declared unauthorised and illegal.¹⁷ SEBI claimed crowdfunding activities as unauthorized and the online platforms contravenes the provisions of private placement.¹⁸ Further, the SEBI notice sent to these platforms for violating the private

¹¹ John Wasik, *Crowdfunding, the JOBS Act, and Scams in Your Inbox*, Forbes (March 23, 2012), <https://www.forbes.com/sites/johnwasik/2012/03/23/potential-and-obvious-scams/?sh=3ae5d2114d2f>.

¹² *SEBI Consultation Paper on Crowdfunding*, SECURITY EXCHANGE BOARD OF INDIA (2014).

¹³ *Borland's Trustee v. Steel Brothers & Co Ltd* [1901] 1 Ch 279, 288.

¹⁴ *Cautions Investors*, SEBI PRESS RELEASE, https://www.sebi.gov.in/media/press-releases/aug-2016/sebi-cautions-investors_33094.html. See also, *SEBI Cautions Investors*, SECURITIES AND EXCHANGE BOARD OF INDIA, https://www.sebi.gov.in/media/press-releases/aug-2016/sebi-cautions-investors_33094.html.

¹⁵ *Crowd control: Sebi warning turns off crowdfunding tap for start-ups*, TIMES OF INDIA, <https://timesofindia.indiatimes.com/business/startups/companies/crowd-control-sebi-warning-turns-off-crowdfunding-tap-for-startups/articleshow/54218934.cms>.

¹⁶ Anirudh Laskar, *SEBI Wants Disclaimer for Crowdfunding*, LIVEMINT (September 8, 2017), <https://www.livemint.com/Money/ic0BUI5NSsO1yeJSNAAP1I/Sebi-wants-crowdfunding-bodies-to-warn-investors.html>.

¹⁷ *SEBI Cautions Investors*, SECURITIES AND EXCHANGE BOARD OF INDIA, PR No. 137/2016, https://www.sebi.gov.in/media/press-releases/aug-2016/sebi-cautions-investors_33094.html.

¹⁸ Pavan Burugula, *Crowd Funding Platforms Rush to SEBI for Alternative Investment Fund Tag*, THE ECONOMIC TIMES (March 1, 2019), <https://economictimes.indiatimes.com/markets/stocks/news/crowd-funding-platforms-rush-to-sebi-for-alternative-investment-fund-tag/articleshow/68213207.cms>. See also, Ayush Wadhi & Swati Shekar, *Equity Crowdfunding in India: Present Perspectives and Prospects* in EMERGING TRENDS IN

placement mandates. Upon receiving the notice, the said platforms rushed to get registration with SEBI as Alternation Investment Fund (“AIF”).¹⁹ It assumes significance to infer two aspects to understand the SEBI’s implicit intention to regulate crowdfunding within the existing regulatory framework. *Firstly*, SEBI expects the crowdfunding platforms to adhere with private placement mandates. *Secondly*, instead of subjecting the violating platforms to the public issue mandates and punish them, SEBI expected the crowdfunding platforms to get registered under AIF. These inferences uncover the SEBI’s implicit intention to regulate crowdfunding through the existing regulatory framework.

Arguably, SEBI’s rationale behind not regulating crowdfunding as public issue would be SEBI’s acknowledgement that public issue involves increased cost of capital in public offer,²⁰ onerous requirements²¹ and eligibility criteria that a start-up venture could not afford. Having understood SEBI’s plausible rationale behind not adopting public issue, the next chapter attempts to analyse the appropriateness of bringing crowdfunding under the regulatory scope of AIF regulations and other regulations.

III. APPROPRIATENESS OF BRINGING CROWDFUNDING IN THE REGULATORY REALM OF OTHER INVESTMENTS

From investors’ perspective, arguably, AIF regulations cannot be applied to equity crowdfunding as most of the contributors to crowdfunding wouldn’t qualify the minimum investment requirements i.e., Rs. 1 Crore.²² Because existing literature uncovers that crowdfunding ventures would typically receive only small investments from various investors.²³ While it is argued that crowdfunding cannot be regulated under AIF regulations, the same cannot be regulated under Venture Capital Fund (“VCF”) and Innovators Growth Platform (“IGP”) as well.

CORPORATE AND COMMERCIAL LAWS IN INDIA 112 (2019). The existing regulations in light of Sahara decision, prohibits the companies from offering shares more than 200 investors in a financial year, without undertaking public offer. *See*, Section 42, Companies Act 2013 r/w Rule 14 and Form PAS-4 of the Companies (Prospectus and Allotment of Securities) Rules 2014; Regulation 2 (ZC), SEBI ICDR Regulation 2009; Rule 14 (2), Companies (Prospectus and Allotment of Securities) Rules 2014. *See also*, Sahara India Real Estate Corporation Ltd & Ors v. Securities Exchange Board of India & Anr (2013) 1 SCC 1.

¹⁹ Regulation 2 (1) b, SEBI (AIF) Regulation 2012.

²⁰ *See*, Jay R. Ritter, *The Costs of Going Public* 19 (2) JOURNAL OF FINANCIAL ECONOMICS 261 (1987).

²¹ *See generally*, SEBI (ICDR) Regulation, 2009.

²² *See*, Regulation 10 (c), SEBI (Alternative Investment Funds) Regulation 2012.

²³ *See for instance*, Gordon Burtch & et al., *An Empirical Examination of the Antecedents and Consequences of Contribution Patterns in Crowd-Funded Markets* 24 (3) INFORMATION SYSTEMS RESEARCH 499 (2013).

Similar to AIF, the participation in VCF requires minimum of Rs. 5,00,000/- as an investment requirement.²⁴ Moreover, the venture capital investors are mostly inapproachable for small entrepreneurs and business²⁵ and venture capital investors invest on less risky companies that would have proven track record.²⁶ While angel funds have relatively liberal regulation, the angel investors would only fill a part of resource gap of a venture. Arguably, mostly such investments would be insufficient for a start-up ventures.²⁷

Besides, arguably, crowdfunding cannot be regulated through the regulatory framework of Innovators Growth Platform (“IGP”). IGP is modified version of Institutional Trading Platform (“ITP”) introduced through SEBI ICDR (Second Amendment) Regulation 2019. The objective of IGP is to enable listing the shares of business with “*substantial value addition*”,²⁸ without public issue²⁹ and mandate of having minimum public shareholding.³⁰ IGP cannot regulated crowdfunding owing to, arguably, a weak investor protection mechanism. Because while it is a *sine qua non* to hold 25% of the pre-issue share capital of the issuer by prescribed sophisticated investors,³¹ IGP regulation is silent about the remaining 75% of the investors, without any investment limits and thereby have weak investor protection.

Therefore, it is inferred that the crowdfunding cannot be regulated within the existing regulatory framework. Therefore, it assumes significance to create a conducive framework for regulating crowdfunding balancing both promotion of entrepreneurship and investor protection. In that line, the upcoming chapters attempt to analyse the effectiveness of the regulatory framework proposed by the SEBI in 2014 through its consultation paper.

²⁴ See, Regulation 11 (2), SEBI (Venture Capital Funds) Regulations 1996. See also, C. Steven Bradford, *Crowdfunding and the Federal Securities Laws* 12 (1) COLUMBIA BUSINESS LAW REVIEW 1, 5 (2012).

²⁵ *Id.*

²⁶ *Response to SEBI Consultation Paper on Crowdfunding*, VIDHI CENTRE FOR LEGAL POLICY (2014), at 2.

²⁷ C. Steven Bradford, *supra* note 30.

²⁸ Regulation 283 (1), SEBI ICDR 2018

²⁹ Chapter X, Part II, SEBI ICDR 2018

³⁰ Regulation 284 (7), SEBI ICDR 2018

³¹ QIB (Regulation 2 (ss), SEBI ICDR 2018; Innovators Growth Platform Investors (Regulation 283 (1) (Explanation), SEBI ICDR 2018).

IV. SEBI'S PROPOSED FRAMEWORK ON CROWDFUNDING

On one hand, it is inferred that SEBI attempts to regulate crowdfunding within the existing regulatory framework of other investment platforms. On the other hand, in order to initiate discussions on the regulatory framework for crowdfunding, SEBI has issued a consultation paper in 2014.³² Seemingly, SEBI's this move aligns with the principles of International Organization of Securities Commission ("IOSCO") which emphasises the regulators duty to identify, monitor & mitigate systemic risk and contribute to regular review of the perimeter of regulation.³³

SEBI's proposed framework restricts the crowdfunding participation to "Accredited Investors" who must have at least Rs. 10 Lakhs annual gross income.³⁴ Besides, the investors are obligated to invest at least Rs. 20,000/-³⁵ and at most Rs. 60,000/- in a crowdfunding issue and such investment must not exceed 10% of the crowdfunding's net worth. The number of investors who can invest in a crowdfunding issue was also capped to the maximum of 200 investors. In order to ensure the adequate disclosure for informed consent, the private placement offer letter must be circulated online by the issuer to the selected accredited investors registered with crowdfunding platforms.³⁶ This proposed framework of the SEBI suffer inherent theoretical and logical flaws that the upcoming chapter attempts to critically discuss.

³² *Consultation Paper on Crowdfunding in India*, SECURITIES EXCHANGE BOARD OF INDIA (2014).

³³ Principle 6 & 7, IOSCO Principles. *See also, Objective and Principles of Securities Regulation*, IOSCO (2017). <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf>.

³⁴ *SEBI Consultation Paper on Crowdfunding*, SECURITY EXCHANGE BOARD OF INDIA (2014), at ¶ 9.1.4.1.

³⁵ The mandate of minimum investment of Rs. 20,000/- emanates from the *Companies (Prospectus and Allotment of Securities) Rule, 2014*. Because SEBI subjected crowdfunding businesses to the said rule. *See, Rule 14 (2)(c), Companies (Prospectus and Allotment of Securities) Rule (2014)*. *See also, Shubhan Kumar Singh, Innovators Growth Platform: NASDAQ of India*, THE CBCL BLOG (May 30, 2021), <https://cbcl.nliu.ac.in/capital-markets-and-securities-law/innovators-growth-platform-nasdaq-of-india/>.

³⁶ *SEBI Consultation Paper on Crowdfunding*, SECURITY EXCHANGE BOARD OF INDIA (2014), at ¶ 9.3.3

V. APPROPRIATENESS OF SEBI'S PROPOSAL TO REGULATE CROWDFUNDING

To critically appraise the SEBI's proposed regulatory framework, the regulatory theories emphasised by Mariene Amstad were employed for analysis. Mariene Amstad highlights three crucial financial regulatory theory viz., "*Ignore* (not regulate), *duck type* (same risk, same rules) or *code* (new functions, new rule)".³⁷

The first theory of finance regulation i.e., "*Ignore*" supports non-regulation of the crowdfunding. However, SEBI seemingly intends to regulate the crowdfunding which could be inferred from the publication of Consultation Paper on Crowdfunding in 2014. Further, the second theory i.e., "*Duck Type*" reflects the regulatory strategy of regulating similar financial functions alike i.e., "*If it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a duck*".³⁸ The similar function-based regulatory approach could be witnessed from the famous *Howey Test*,³⁹ where the definition of "*securities*" was based on investment's substance (function) rather than its form.⁴⁰ Under the third theory i.e., "*Code*" the regulator would create new regulations if there arise new functionality from the fintech.

In the instant case of regulating crowdfunding, arguably, SEBI adopts duck-type approach. Because, the SEBI's proposed framework required the start-ups to comply with the process of standard private placement with minor changes.⁴¹ Having adopted the duck-type approach of regulation, arguably, there exists two conundrums viz., Ignoring the '*New functionality*' and thereby violating the principle of proportionality, that the next chapter attempts to discuss.

³⁷ Mariene Amstad, *Regulating fintech: Ignore, duck type, or code*, VOX EU (March 21, 2019)

<https://cepr.org/voxeu/columns/regulating-fintech-ignore-duck-type-or-code#:~:text=Duck%2Dtyping%20regulates%20the%20function,that%20specifically%20address%20fintech%20issues>. See also, Mariena Amstad, *Regulating Fintech: Objectives, Principles and Practices*, ADBI WORKING PAPER SERIES (2019), <https://www.adb.org/sites/default/files/publication/533791/adbi-wp1016.pdf>.

³⁸ Mariena Amstad, *Regulating Fintech: Objectives, Principles and Practices*, ADBI WORKING PAPER SERIES (2019), <https://www.adb.org/sites/default/files/publication/533791/adbi-wp1016.pdf>.

³⁹ SEC v. W.J. Howey Co., 328 U.S. 293 (1946), at 293 & 301.

⁴⁰ Mariena Amstad, *supra* note 43, at n 17.

⁴¹ See, Nidhi Agarwal, *supra* note 9.

VI. TWIN CONUNDRUMS IN ADOPTING DUCK-TYPE APPROACH

The proposed regulatory framework by the SEBI to regulate crowdfunding essentially failed to address the new functionality and object of ‘*Crowdfunding*.’”

Because the idea of crowdfunding is based on the principle of “*Wisdom of the Crowd*” i.e., crowd has wisdom and ability to make good investment.⁴² Though not every person would be well-informed about proper investments, theoretically, a crowd can still collectively arrive at a wise decision.⁴³ The behavioural psychology discourse also suggests that the crowd would make choices depending on the previous (or earlier) decision maker.⁴⁴ Literature on crowdfunding claims that the knowledge gap between professionals and the general public has struck due to readily available internet sources.⁴⁵ The IOSCO also emphasis this “*wisdom of the crowds*” in website design with quoted example of EBay and Wikipedia.⁴⁶

In this light, IOSCO principles also highlights three type of regulatory regime viz., (1) regulation banning equity crowdfunding; (2) regulation creating high entry barrier; (3) enabling equity crowdfunding to only sophisticated investors. Inferably, SEBI have adopted the last approach, which is arguably against the principle of proportionality. Principle of Proportionality aims at limiting high regulatory duties to curb excessive cost of compliance and regulatory burden for smaller start-ups.⁴⁷ In this regard, the Jumpstart Our Business Start-up Act (JOBS Act) of United States of America, that provides specific crowdfunding exemption could be taken for policy comparison.⁴⁸ The Act imposes conditional small issue exemption⁴⁹ to the issuer and investment threshold to the investors. If the Securities Exchange Commission (SEC) recognize one as accredited investor,⁵⁰ no maximum threshold

⁴² Ayush Wadhi & Swati Shekar, *Equity Crowdfunding in India: Present Perspectives and Prospects* in EMERGING TRENDS IN CORPORATE AND COMMERCIAL LAWS IN INDIA 112 (2019).

⁴³ C. Streven Bradford, *supra* note 12.

⁴⁴ Heminway, Joan MacLeod, *Investor and Market Protection in the Crowdfunding Era: Disclosing to and for the “Crowd”* 38 VTLR 827 (2014).

⁴⁵ JEFF HOWE, CROWDSOURCING: WHY THE POWER OF THE CROWD IS DRIVING THE FUTURE OF BUSINESS 39-40 (2008).

⁴⁶ Eleanor Kirby & Shane Worner, *Crowd-funding: An Infant Industry Growing Fast*, IOSCO 12 (2014).

⁴⁷ Basel Committee on Banking Supervision (BCBS) 2019.

⁴⁸ This legislation was introduced in USA in the year of 2012. *See*, DLA Piper, *JOBS Act Passes Congress, HEADS TO WHITE HOUSE FOR SIGNATURE* (Mar. 28, 2012), <http://www.dlapiper.com/jobs-act-passes-congress-heads-to-white-house-for-signature/>.

⁴⁹ Regulation A, § 230.251 (a), Jumpstart Our Business Start-up Act 2012.

⁵⁰ *See*, Rule 506 of Regulation D.

on the investment is vested. Rather, non-accredited investors were capped with maximum threshold of investment based on their annual income.⁵¹

However, in SEBI's proposed regulatory framework, there is high threshold of accreditation and eligibility for retail investor is, arguably, against the core tenets of crowdfunding *i.e.*, to enable investors participate in investment who otherwise wouldn't have engaged in conventional capital market. Also, arguably, the threshold on maximum investment (*i.e.*, INR 60, 000/-) is baseless as it is not based on objective-cum-equitable factors such as '*Individual investors*' income. Further, practically, it is unlikely that QIBs will invest in a start-up with no track record.⁵² The maximum cap of 200 shareholders again runs contrary to the idea of crowdfunding.⁵³ Therefore, these regulations suggested by SEBI are, arguably, seemingly impractical, unproportional, and against the spirit of crowdfunding.

VII. CONCLUDING REMARKS

Having understood the need for regulating the equity crowdfunding in India, SEBI has published the Consultation paper in 2014. However, no concrete regulatory move has been witnessed, apart from SEBI's measures to make the public issue requirement flexible for start-ups such as Innovators Growth Platform. However, analysis reveals that regulating crowdfunding under the existing regulatory framework would be inefficient. However, SEBI has proposed a "*Duck-type*" approach to regulate crowdfunding under the framework of private placement (with some exemptions). Having proposed that such an approach ignores the new functionality of crowdfunding and fall foul of the proportionality principle. Therefore, it is suggested that SEBI may adopt a "*Code (new function, new rule)*" approach to regulating crowdfunding with no investor threshold but with an investment threshold in proportion to the investor's risk-bearing capacity. Thereby, the accredited investors may not be imposed with any investment threshold. Further, the non-accredited investors may be enabled to invest in crowdfunding, and to ensure investor protection, the same shall be subject to the maximum investment threshold dependent on the annual income of the retail investor (which would determine the risk-bearing capacity of the investors). Besides, the

⁵¹ § 302, The JOBS Act 2002. *See also*, *Updated Investor Bulletin: Regulation Crowdfunding for Investor*, SEC (October 14, 2022), <https://www.sec.gov/oiea/investor-alerts-bulletins/ib-crowdfunding>.

⁵² C. Streven Bradford, *supra* note 12.

⁵³ Whereas, in JOBS Act, exclusion of crowdfunding investors from the share-holder cap has been explicitly given. *See*, § 303, JOBS Act 2012.

threshold of a number of shareholders shall be scrapped, as the blanket investment limit and restricting the entry to non-accredited investors serves to be an anti-thesis to the idea of crowdfunding to engage the public at large to raise finance for start-up companies. Towards this, the JOBS Act of the US could be taken for policy consideration.

However, since share is primarily a liability, mitigating the risk is cardinal and while doing so, there ought to be a balance between investor protection and the promotion of entrepreneurship. Disproportionate regulation to ensure investor protection would cost the benefit of crowdfunding. Thereby, the risk that the start-ups would take is relatively fringe which has to be balanced with appropriate disclosure.⁵⁴ In this context, the IOSCO suggests that “*Disclosure to retail investors...is important along with consideration of suitability.*” From the perspective of law and economics, the behavioural economics reveals the biases that affects effective investment-decision making such as overconfidence,⁵⁵ illusion of control, halo effect and anchoring etc. However, these cognitive biases may be mitigated through nudges based on visibility of incentives of the risk of loss.⁵⁶ In this line, SEBI has proposed to mandate the disclosure requirement in the standard of a private placement offer letter.⁵⁷ This seemingly gives the investors the caution about the prospective risk that they would undertake by subscribing to the equity through crowdfunding. This aligns with the principle 16 of IOSCO i.e., “*There should be a full and timely disclosure of financial results, risk and other information material to investor’s decision making.*”⁵⁸ Having said that, the detailed analysis on the effectiveness of disclosure requirement for risk mitigation in crowdfunding serves to be the future scope of the study.

⁵⁴ Eleanor Kirby & Shane Worner, *Crowd-funding: An Infant Industry Growing Fast*, Staff Working Paper No. [SWP3/2014], IOSCO RESEARCH DEPARTMENT 50 (2014).

⁵⁵ See also, *Behavioural Economics for Investor Protection- Practical Recommendations for Investors, Entities and Regulators*, COMISION NACIONAL DEL MERCADO DE VALORES (May 22, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606264.

⁵⁶ See, *Behavioural Economics for Investor Protection- Practical Recommendations for Investors, Entities and Regulators*, COMISION NACIONAL DEL MERCADO DE VALORES (May 22, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606264.

⁵⁷ *SEBI Consultation Paper on Crowdfunding*, SECURITY EXCHANGE BOARD OF INDIA (2014), at ¶ 9.3.3.

⁵⁸ *Objective and Principles of Securities Regulation*, IOSCO (2017).
<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf>.

VIII. CONCLUSION

It is reasonable to conclude that CBDCs have much potential based on analysing different cases and characteristics. They could ultimately overtake other financial transactions as the preferred method for individuals and companies. Additionally, the CBDCs would continuously alter the established financial sector precedents. CBDC use cases may significantly alter how individuals and organisations see digital currency.

While there is still much debate over whether CBDCs are necessary or even desirable, several countries are actively exploring the possibility of issuing them. India is one such country, and its recent announcement that it is working on a CBDC has attracted a great deal of attention.

A significant number of resources will need to be invested in creating and operating a retail CBDC. In-depth user behaviour analysis is essential in addition to conducting pilots so that it can guide how a CBDC is created and promoted for broad adoption. However, the development of CBDC presents some challenges which need to be addressed before the final launching of CBDC in India. If the issues are not avoided, they might prove to be fatal in the Indian economic space and would also lead to uncontrollable inflation.

New legislation, which is made considering technological advancements, is the need of the hour. Only when new technologies are utilised to implement rules and prevent different attacks on digital currency can the launch of CBDC succeed.

CRIMINAL LIABILITY OF ARTIFICIAL INTELLIGENCE

~Prakruti N¹

I. INTRODUCTION

In Austin, Texas, a group of protestors handed out “stop the robots” shirts in March 2015.² While it’s no doubt that intelligent robots are extremely useful, these protestors also believed that they could be extremely dangerous and further scientific development in the field should be done with extreme caution with specific focus on ensuring that these developments should be done safely.

In the 21st century, technology seems to be developing in an exponential rate. This development is so rapid that older generations often find themselves unable to catch up with the latest technology. Along with them, our laws and policies find themselves outdated or insufficient from time to time.

In 1969 the ARPANET network was invented, which was the first network to run on the TCP/IP protocol suite.³ In 1989 the World Wide Web (WWW) was born⁴. It took another decade after this for India to introduce the Information Technology Act.

AI is the capability of a machine to mimic intelligent human behavior. This allows the bot to function autonomously. While acting autonomously, a robot could cause injury or commit an act which would be criminal if committed by a person. In such cases, who is liable for such an act?

The Indian Penal Code defines “Person” as- The word “person” includes any Company or Association or body of persons, whether incorporated or not. It does not recognize AI as a person, and further has no provisions to determine who is liable for the actions of AI.

This research paper contains some models of determining liability from all over the world and analyses each one of them with respect to its relevance and applicability in India.

¹ The author is in her 3rd year studying at Maharashtra National Law University, Mumbai.

² Miller, R. (2015) Anti-robot protest held at SXSW, TechCrunch, <https://techcrunch.com/2015/03/14/anti-robot-protest-held-at-sxsw/>

³ Cox, K. *A brief history of network technology, trueCABLE*. Available at: <https://www.truecable.com/blogs/cable-academy/a-brief-history-of-network-technology>

⁴ *History of the web* (no date) World Wide Web Foundation. Available at: <https://webfoundation.org/about/vision/history-of-the-web/>

Hallevy Models

Gabriel Hallevy⁵ has identified three liability models for offenses committed by AI.

1. The Perpetration-by-Another Liability Model

This is the simplest liability model. Primitive AI machines have decision making capabilities, but such capabilities are confined to its algorithm. These algorithms are straightforward to the extent that it has no black-box⁶ effect.⁷ In these cases, an AI is simply viewed as an innocent-agent.

However, it is important to note that in this model, an AI system is not simply equated with a non-intelligent machine, but rather equated to a mentally limited person, such as a child. This model is compatible with the existing provisions of the IPC.

According to S.108 of the IPC⁸, an abettor is a person who abets either the commission of an offence, or *the commission of an act which would be an offence, if committed by a person capable by law of committing an offence* with the same intention or knowledge as that of the abettor.

The definition of a person is not limited to, but inclusive of an association, company or body of persons. The distinction between simple robots and AI robots is drawn using the fact that AI robots have the capacity to mimic human intelligence and take independent decisions. This could potentially be enough grounds to also classify them as a 'legal person'. Such an inclusion is neither ground breaking, nor bizarre in light of the fact that Sophie, an AI robot was given the Saudi Arabian citizenship.

Further, in explanation 3 it is stated that "It is not necessary that the person abetted should be capable by law of committing an offence, or that he should have the same guilty intention or knowledge as that of the abettor, *or any guilty intention or knowledge.*"⁹. An AI robot does not need to possess mens rea, or even have the capacity to possess such mens rea

⁵ Hallevy, P.G. (2019) "The basic models of criminal liability of AI systems and Outer Circles," *SSRN Electronic Journal* [Preprint]. Available at: <https://doi.org/10.2139/ssrn.3402527>.

⁶ A 'black box' is a device, system or program that allows you to see the input and output, but gives no view of the processes and workings between. The AI black box, then, refers to the fact that with most AI-based tools, we don't know how they do what they do

⁷ Reed, N. (2021) *The Ai Black Box Problem*, *ThinkAutomation*. Available at: <https://www.thinkautomation.com/bots-and-ai/the-ai-black-box-problem/>.

⁸ Indian Penal Code, § 108, Acts of Parliament, 1860 (India)

⁹ *Supra*, note 5.

in order to have been abetted in a crime.

In this liability model, either the programmer or the user can be made liable depending on the origin of the perpetration. If the programmer, in the code of the robot, programmed the robot to behave in such manner that a law would be broken, he would then be held liable (as an abettor or perpetrator). For example, if a programmer creates a robot to generate automated responses in the customer service section of a particular retail website and includes in its program certain responses that could amount to sexual harassment, he could be liable for abetment of sexual harassment. However, if the code was innocent but the user used the innocent code to instruct the robot to do something that could potentially violate a law, then he would be liable.

However, an AI robot is not always an innocent agent. Sometimes an AI does an act that is against the law or harmful to another person, even though it isn't specifically programmed to do so. In such cases, no other human being has mens rea or actively contributes to the actus reus. In these cases, the previous model will fail.

2. The Natural Probable Consequence Liability Model

When an AI robot does an act which it wasn't explicitly programmed to do, which in turn amounts to any crime under the IPC, the liability will depend on the foreseeability of the crime.

For example, if a pilot is flying a plane and decides to turn on automatic pilot mode, an AI entity will begin to control the plane, much like a human pilot. The pilot gets news of a sudden change in weather and realizes a storm is brewing on the path the AI entity was planning to take. The pilot then tries to change the course of the plane which the AI entity sees as a threat to the safety of the plane. As a response, it decides to eject the pilot from his seat, thereby killing him.

The plane was never specifically instructed to kill anyone, much less a pilot. Machine learning allows a robot to access a large amount of data and learn from it. This data is unfiltered and the entity can learn virtually anything without the supervision of a human. It is possible that no human being had the knowledge that the AI robot had the requisite knowledge to eject a pilot from the plane.

However, the auto pilot function had not been specifically restricted from ejecting a human. In the natural course of the auto pilot's functions, it was likely that it learnt to protect the plane from external dangers by way of ejection, cutting off oxygen supply etc. Here, there is no intention of the programmer or user to kill the pilot, but the mere negligence in this model amounts to mens rea.

When an AI entity is created, the programmer and the user must be able to foresee all natural and probable consequences of the algorithm and ensure that these are protected against. The programmer in this case should have ensured that the AI doesn't harm a person, especially the pilot, much less cause his death. Machine learning can be infinite, so the onus of adding checks and balances lies on the programmer.

In context of the Indian legal system, vicarious liability regime can be expanded to be applied here. Under vicarious liability, a parent is vicariously liable for the actions of their child. At the same time, a master is liable for the acts of their servant. The programmer shares a parental role towards the AI entity while the user has a master-servant relationship with the AI entity.

Both the programmer and the user must constantly be mindful of the natural and probable consequences of their use of the AI entity.

II. DIRECT LIABILITY

In the first scenario, a robot was viewed as an innocent agent. However, in the second scenario the AI entity is not treated as a child or a mentally ill person. The only differentiating factor between AI and human is *mens rea*. However, not all crimes require intention. In these cases, if an AI entity violates a law and the elements of that crime are fulfilled, the defence that AI does not possess mens rea cannot be used. However, Hallevy, at this point, emphasises that liability of an AI entity is additive in nature and does not substitute the liability of the person.

There are other liability models that can be employed to determine liability.

III. PRODUCT LIABILITY

"Product liability" is the responsibility of a product manufacturer or product seller, to compensate for any harm caused to a consumer by a defective product manufactured or sold or by deficiency in services relating thereto.¹⁰

When Google, and then Volvo and other car manufacturers released their self-driving cars, the liability of car accidents mostly fell upon the manufacturers. This is because these AI systems were considered to be a product purchased by the user and the manufacturer would be liable for the malfunctioning of such product.

However, product liability is a very niche liability model and can only be applied for those AI entities with highly specific use cases. Further, it only deals with civil liability and compensation, not criminal liability.

IV. STRICT LIABILITY

In theory, it seems fair that *Mens Rea* should be taken into consideration while determining the liability of a crime committed by an AI entity, especially when *Mens Rea* is a requisite element of that crime. However, it is true that robots are incapable of possessing such mens rea. When a machine learning AI robot is purchased or created, the onus of preventing such a dangerous object from causing hurt to someone lies on the owner of the AI entity.

The elements of strict liability are:

- Dangerous thing:

Artificial Intelligence is unpredictable. Coupled with this, it can also be physically stronger than a human. It has better computing power than a human. Unfortunately, it is also prone to making mistakes and lacks the basic morals and ethics of a human. In Japan, Kenji Urada was killed by a robotic arm as it mistook his identity and failed to recognise that he wasn't an intruder. Such mistakes are not made by the average human being which makes robots specifically dangerous.

¹⁰ Consumer Protection Act, 2019, § 2, NO. 35, Acts of Parliament, 2019 (IN)

- Unnatural Land Use

In the case above, the robot was stationed in a factory which isn't unnatural land use. Neither is using self-driving cars. However, if one was to purchase a huge AI gadget for their backyard which then attacked a neighbour thinking of said neighbour to be a threat, this kind of use could amount to unnatural land use.

- Escape

This escape need not necessarily be physical. As long as the escape means going out of the control of the owner, any act done by the robot, outside what the owner intended to make the robot do, can be construed as an escape. However, both these elements are far-fetched as in most cases robots are used for very natural land uses.

A European Commission report states that “A person operating a permissible technology that nevertheless carries an increased risk of harm to others, for example AI-driven robots in public spaces, should be subject to strict liability for damage resulting from its operation”¹¹ However, there is no similar legislation in India to introduce strict liability to AI.

Currently, AI is either treated like a product, or a dangerous animal, a child or an actual human being. However, AI itself is a vast subject with many different subsets of differing sophistications. While most primitive AI entities only act as innocent agents, more sophisticated machine learning AIs even have the capability of being perpetrators.

Robots learn from not just unfiltered data but also patterns. This means that they are not only capable of learning information, but also the human biases that are intertwined with it. Robots are only getting more and more sophisticated and it is high time that our laws recognize the same.

A company can be considered a person and held liable for the acts of itself. Though a company is not an actual person, the laws don't only individually hold the members of the company's board liable. In the same way, the definition of person can be expanded to include AI entities. Or, a new definition can be incorporated to do the same.

Robots are capable of causing dangerous accidents. Sometimes they are coded improperly which results in them doing a wrongful act. If such robots are recognized to be dangerous,

¹¹ *Liability for Artificial Intelligence - European Parliament.* Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/

holding them liable could allow the courts to put down these robots or prevent the manufacturer from making more of such dangerous robots. Robots can inherit the ugly biases of humanity. Microsoft's AI chatbot Tay interacted with people for less than 24 hours on twitter before tweeting questionable and offensive tweets. While Microsoft claimed that this chatbot was filtered before release, in less than a day it was evident that this bot had no (or not enough) filters.¹²

If this bot was held to be liable for hate speech, it could be possible for the courts to order the bot to be shut down and never sold again. Criminal liability of AI may have no retributive effect (yet) but it still has some preventative effect.

V. CONCLUSION

Artificial Intelligence is developing at a fast pace but our laws are under equipped to deal with these entities. Currently, our courts have no choice but to make do with existing statutes to determine the liability of AI. However, the IPC catch up to the existing technology soon and define a clear set of rules to deal with the liability of Artificial Intelligence.

As AI is an ever-evolving field, and what we find ourselves in is just the beginning, our lawmakers must also keep an eye on the future and draft the laws to accommodate further advancements in AI and possible legal challenges they might pose.

¹² Wendehorst, C. (2020) *Strict liability for AI and other emerging technologies*, De Gruyter. De Gruyter. Available at: <https://www.degruyter.com/document/doi/10.1515/jetl-2020-0140/html?lang=en>.

DIGITAL TRANSACTIONS AND THE RISE OF CYBERCRIMES: TESTING THE READINESS OF THE INDIAN LEGAL STRUCTURE

~ Dwija Vasavada & Diya Gohil ¹

ABSTRACT

In the era of digitalization, the Indian economy has witnessed a major upturn with the help of breakthrough policies and digitally-backed structures that have eased the lives of millions of nationals of the country. With a swipe, a hefty sum of money can be transferred from one remote area of the county to another within a fraction of a second. This trend in the techno- digital world has made everyone well-versed in terms like "e-banking," "e-commerce," "e-networking," etc., wherein the angle of preference or choice is greatly bent towards the mode that is easily accessible and attainable. But with the increase in the number of users of such digitally driven systems, it is equally important to regulate such platforms by framing stringent laws to protect the fundamental right to privacy of the users against the misuse of the sensitive information that has been shared by them with a sense of utmost reliance. Therefore, considering all the outlining aspects of an economy that is at the peak of automation, the authors in this article aim to deeply analyze the legalities that revolve around the digital economy concerning the digital payment systems of the country to identify the drawbacks in the governance of such laws that regulate it. The article begins with an overview of the online transaction system, which has flourished primarily since the pandemic, and then sheds some light on the potential cybercrimes that have been increasing with technological advancement. It further discusses the current legal system by identifying specific loopholes, and lastly, the authors provide relevant findings and suggestions and analyze international jurisdictions that have been in conflict with the "digitalization of crimes" to counter the menace of the spurt of cybercrimes and the drawbacks of the Indian legal structure.

¹ The authors are in their 2nd Year at Gujarat National Law University and United World School of Law.

I. UNDERSTANDING E-TRANSACTIONS AND THE INDIAN DIGITAL ECONOMY

It should not come as a surprise that the world's fifth-largest economy is leading and advancing global digital wealth, but what is noteworthy is the significant surge that has occurred in such a short span of time. The term "digital economy" describes how the digital revolution is replacing conventional brick-and-mortar activities. The transformation has not only altered people's fundamental way of life but has also played an important role in raising their standards of living. Many sectors of the economy have witnessed notable changes as a result of digital advancement, including medicine, education, banking, and the service sector, among many others.

The Government of India launched the Digital India Campaign in 2015 to empower the nation digitally and improve the online infrastructure of the Indian economy. The Unified Payments Interface (UPI) portal was created by the National Payments Corporation of India (NPCI), an initiative of the Reserve Bank of India, to expedite and streamline digital transactions. The portal facilitates interbank real-time transactions via mobile applications such as Bharat Interface for Money (BHIM), Google Pay, Paytm, PhonePe, and others. Even in the midst of the Indian economy's deteriorating conditions, this inclusive digital model of India contributed to closing the digital divide and bringing the advantages of technology to all facets of the population. Hence, it is important to use digitization as the primary factor of production to establish a sound digital economy.

The era of digital transactions in India began in 1996 when banks started offering online banking services through electronic banking at their branches. Later, as more banks launched net banking services, the trend accelerated. Technology was already playing a bigger role in the workforce, but it was not until the pandemic that a complete reliance on the digital economic setup was seen. Due to the impact of COVID-19, the banking, education, healthcare, and food delivery sectors have grown rapidly. And since then, there has been a significant increase in the number of users of "e-transactions" in India.

The outbreak of the novel coronavirus and the prohibition against in-person business meetings significantly hastened the adoption of these technologies. With the rise in the number of coronavirus cases, digital transactions have become more common. From a tea vendor to a large corporation, everyone has recognized the value of digitization and, as a

result, has adopted the digital method. In light of this, it can be said that even though the nationwide lockdown was upsetting, Indian electronic payment systems have turned out to be a blessing in disguise.

II. CYBERCRIMES IN INDIA AND THE GROWTH TRAJECTORY

The prevalence of cybercrime has indeed increased with the rise of digital technology. The transition from traditional work culture to digital operations has brought numerous benefits and innovations, but it has also introduced new vulnerabilities and threats to cybersecurity. The interconnected nature of digital systems and the growing reliance on technology for various aspects of our lives have provided cybercriminals with more opportunities to exploit weaknesses and carry out malicious activities. These activities can range from stealing sensitive personal information and financial data to launching large-scale cyberattacks on organizations and even governments.

The history of cybercrime in India can be traced back to the early days of the Internet. In the late 1990s and early 2000s, India's internet penetration was still relatively low, and cybercrime was largely limited to hacking and unauthorized access to computer systems. These early cybercriminals were often motivated by curiosity or a desire to showcase their technical skills. India's internet usage increased along with the rise in cybercrime incidents.

In the mid-2000s, incidents of online fraud and identity theft started to increase. These crimes were frequently carried out by lone perpetrators or small groups using simple tools and techniques. In the late 2000s and early 2010s, as social media and mobile technology grew in popularity, a new set of cybercrime challenges emerged. Social media platforms became breeding grounds for cyberbullying, online harassment, and the spread of misinformation.

In 2013, India witnessed its first cybercrime conviction following a complaint filed by Sony India Private Ltd. The case of *Sony Sambandh*² involved a fraudulent transaction made on a website targeting non-resident Indians. The accused gained access to an American national's credit card number while working at a call centre and misused it on the website to purchase a Sony television set and cordless headphones. The company delivered the products to the accused, but it was later discovered that the transaction was unauthorized. Sony lodged a

² Avni Mishra, *A primer on cybercrimes*, 2 JUS CORPUS LAW J. 12 (2021), <https://www.juscorpus.com/wp-content/uploads/2021/09/3.-Avni-Mishra.pdf>.

complaint, and the Central Bureau of Investigation (CBI) registered a case under Sections 418³, 419⁴, and 420⁵ of the Indian Penal Code, 1860.

The Court found the accused guilty and convicted him under the relevant sections of the Indian Penal Code, 1860⁶, marking the first conviction in a cybercrime case in India. Despite this, considering his young age and first-time offense, the Court released the accused on probation for one year. The judgment holds significance as it demonstrates the effective application of the Indian Penal Code to certain cybercrimes not covered by the Information Technology Act, of 2000⁷, and sends a strong message that the law cannot be disregarded.

In another such incident, in August 2018, Cosmos Bank in Pune, India, fell victim to a bold cyberattack in which Rs 94 crores were stolen. The hackers managed to breach the bank's main server and transfer the stolen funds to a bank in Hong Kong. Additionally, they infiltrated the ATM server to gather information from VISA and Rupay debit cards. The attack targeted the switching system, which acts as a link between the centralized system and the payment gateway. This prevented the bank and account holders from detecting fraudulent money transfers. This attack was unique and notable as it involved the first malware attack that disrupted all communication between the bank and the payment gateway, enabling the hackers to execute their fraudulent activities without raising suspicion⁸.

These cases highlight the evolving sophistication of cybercrime in India and the need for robust cybersecurity measures to protect individuals, organizations, and the government. As technology continues to advance, it is crucial to stay vigilant and adapt security frameworks to address emerging cyber threats.

With the rapid advancement of technologies like artificial intelligence, blockchain, and the metaverse, cybercrime has also become more sophisticated and organized. Hackers are leveraging these technologies to commit online crimes and exploit vulnerabilities in digital systems.

The use of artificial intelligence by cybercriminals is a concerning trend. They can employ AI to enhance the effectiveness of their attacks, generate targeted phishing emails, spread

³ The Indian Penal Code, 1860, § 418, No. 45, Acts of Parliament, 1860 (India).

⁴ The Indian Penal Code, 1860, § 419, No. 45, Acts of Parliament, 1860 (India).

⁵ The Indian Penal Code, 1860, § 420, No. 45, Acts of Parliament, 1860 (India).

⁶ The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).

⁷ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

⁸ About Us et al., *Important Cyber Law Case Studies*, Cyber Laws & Information Security Advisors 4 (2019), <https://www.cyberalegalservices.com/detail-casestudies.php>.

malware, and collect valuable information by leveraging stolen personal information or open-source data. This demonstrates the need for robust cybersecurity measures to counteract the malicious use of AI.

Espionage and cyberattacks pose significant threats to national security and diplomatic relations for governments. As the concept of Central Bank Digital Currency (CBDC) gains attention, there are specific risks associated with third-party involvement in its implementation. Professionals need to understand the evolving landscape of digital finance to mitigate these risks and protect financial systems from cybercriminals.

The rise of e-currencies and digital payment methods has also led to an exponential increase in digital payment and banking fraud. Cybercriminals target online banking, impersonate bank officials, and exploit vulnerabilities to dupe customers and steal their personal and financial information. The occurrence of frauds involving Aadhar scams and online scams demonstrates the need for improved security in digital transactions and banking services.

Government portals and websites that handle sensitive data are also at risk of being hacked and misused. Cybercriminals can exploit vulnerabilities in these platforms and commit fraud involving debit and credit cards, digital signatures, and electronic contracts. This poses a threat not only to security but also to the confidence of individuals who rely on online activities.

To combat cybercrime effectively, India's legal and security frameworks must keep pace with the evolving landscape of technology. It is crucial to implement robust measures to control and monitor digital platforms, ensuring adherence to cybersecurity standards for privacy and safety. By prioritising cybersecurity and adopting proactive measures, individuals and organisations can mitigate the risks posed by cybercrime and protect sensitive information online.

III. DEVELOPMENT OF LAWS TO REGULATE E-TRANSACTIONS AND POTENTIAL CRIMES

In 2022, India clocked about 70 billion payment transactions, which is the highest in the world, and research by NPCI and People Research on India's Consumer Economy showed that one-third of Indian households are now using digital payments in one way or another⁹.

⁹Mahua Venkatesh, *India tops world ranking in digital payments*, Indianarrative, Oct. 19, 2022, <https://www.indianarrative.com/economy-news/india-tops-world-ranking-in-digital-payments-62451.html>.

Such an increase in digital payments and internet penetration is unavoidable, but with a growing concern about cybercrime in India and around the world, it is essential to formulate policies and enact legislation that prevent the spread of such offenses.

To prevent the abuse of one's integrity, financial institutions that operate digitally need effective cyber laws. As a result, it becomes increasingly important for the Indian legal system to evolve continuously to meet the challenges posed by cybercrime and keep up with its changing nature. In India, there are several cyber laws and regulations in place to curb and regulate digital transactions and potential Internet crimes. Here are some key pieces of legislation that address these issues:

- 1. Information Technology Act, 2000¹⁰ (IT Act):** This is the primary legislation governing cyber activities in India. The statute establishes the rules for data protection and aims to give people more control over their personal information, including the right to be forgotten. It provides legal recognition for electronic transactions, digital signatures, and electronic records. The IT Act also defines various cybercrimes and their penalties, such as unauthorized access, hacking, identity theft, phishing, cyberstalking, and distributing obscene materials online.
- 2. The Indian Penal Code, 1860¹¹ (IPC):** While not specific to cybercrimes, the IPC has provisions that can be applied to online offenses. Sections such as 419¹² (cheating by personation), 463¹³ (forgery), 464¹⁴ (making a false document), 465¹⁵ (forgery), and others can be invoked for cybercrimes.
- 3. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021¹⁶:** These rules, issued under the IT Act, govern the functioning of intermediaries, social media platforms, and digital content providers. They prescribe obligations such as content takedown, the appointment of grievance officers, and disclosure of the originator of objectionable content.

¹⁰ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

¹¹ The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).

¹² The Indian Penal Code, 1860, § 419, No. 45, Acts of Parliament, 1860 (India).

¹³ The Indian Penal Code, 1860, § 463, No. 45, Acts of Parliament, 1860 (India).

¹⁴ The Indian Penal Code, 1860, § 464, No. 45, Acts of Parliament, 1860 (India).

¹⁵ The Indian Penal Code, 1860, § 465, No. 45, Acts of Parliament, 1860 (India).

¹⁶ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

4. **The Payment and Settlement Systems Act, 2007¹⁷:** This statute governs digital payments and provides the legal framework for electronic funds transfer, the regulation of payment systems, and the establishment of payment system operators in India.
5. **The Reserve Bank of India (RBI) Regulations:** The RBI issues various regulations to govern digital transactions, including guidelines for electronic wallets (Prepaid Payment Instruments), online banking, and online payment gateways such as Know Your Customer (KYC) Guidelines¹⁸, Two-Factor Authentication (2FA), etc. These regulations aim to ensure the security and integrity of digital transactions.
6. **The Aadhaar Act, 2016¹⁹:** The Aadhaar Act establishes a unique identification system in India called Aadhaar, which provides a unique identification number to residents. It governs the collection, storage, and usage of Aadhaar-related data and aims to prevent identity-related fraud and misuse.
7. **The Digital Personal Data Protection Bill, 2022²⁰:** The Union Government of India has introduced a revised version of the personal data protection bill, now known as the Digital Personal Data Protection Bill, 2022. Unlike the previous version, this bill allows for cross-border data transfers, instead of mandating local storage of data within India. It takes a more flexible approach to data localization requirements and permits data transfers to specific international destinations, potentially promoting trade agreements between countries. Additionally, the bill acknowledges the right to post-mortem privacy, allowing individuals to withdraw consent even after their death, a provision that was missing in the previous 2019 bill but was recommended by the Joint Parliamentary Committee (JPC).

These are some of the key cyber laws and regulations in India that aim to curb and regulate digital transactions and potential Internet crimes. These are put in place to protect individuals from the unauthorized collection, use, and dissemination of their personal information. Data

¹⁷ Payment and Settlements System Act, 2007, No. 51, Acts of Parliament, 2007 (India).

¹⁸ Reserve Bank of India, Master Directions on Know Your Customer, RBI/DBR/2015-16/18 (Issued on May 29, 2019).

¹⁹ The Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016, No. 47, Acts of Parliament, 2016 (India).

²⁰ Draft Digital Personal Data Protection Bill, 2022, PRS INDIA (2022), <https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022>.

privacy regulations mandate that organizations follow appropriate security measures and procedures to safeguard sensitive personal data or information in accordance with data privacy regulations.

IV. CYBERSECURITY IN LINE WITH THE FINTECH SECTOR

The emergence of FinTech (financial technology) in recent years has created new difficulties for data security and privacy. It is of utmost importance for the concerned governing authorities of the respective jurisdictions to make regulations for the same because fintech companies frequently collect and use large amounts of personal and financial data, making them a prime target for fraudsters.

The financial regulatory landscape in India is characterised by fragmentation, with different regulatory bodies overseeing different aspects of the industry. Fintech companies, despite having limited capital, face regulatory risks that could potentially lead to their collapse or dependence on larger institutions. The Reserve Bank of India (RBI), as the central bank, has emphasised its customer-centric approach to regulation. Various regulatory institutions, including the RBI, SEBI, IRDA, the Ministry of Electronics and Information Technology, and the Ministry of Finance, have developed rules and regulations to govern the product offerings of fintech entities.

While the RBI has released a detailed cybersecurity framework²¹, it currently applies only to banks and non-banking financial institutions. The Working Group²² established by the RBI has identified the need to safeguard customers from unethical practices and the potential stability risks associated with the rapid expansion of digital lending during the pandemic. The group examined issues related to the collaboration between the RBI and other fintech companies offering services such as digital payment systems and "Buy Now, Pay Later" schemes. To protect customer confidentiality and comply with data secrecy obligations, the RBI has issued master directives on the outsourcing of IT services²³ for prepaid payment instructions, and credit-debit cards, which apply to non-banking financial companies (NBFCs) and credit information companies (CICs).

²¹ Reserve Bank of India, Cyber Security Framework in Banks, (Notified on June 2, 2016).

²² Reserve Bank of India, Report of the Working Group on digital lending including lending through online platforms and mobile apps, (Issued on November 18, 2021).

²³ Reserve Bank of India, Draft Master Direction on Outsourcing of Information Technology (IT) Services, (Issued on June 23, 2022).

The regulatory bodies have formulated key rules to effectively regulate fintech companies. The Payment and Settlements Act, 2007²⁴ (PSS Act) is the principal regulation governing payments in India, encompassing various payment systems such as debit cards, credit cards, smart cards, and money transfer systems. Additionally, the RBI has issued circulars and notifications outlining requirements for data localization and data privacy for Payment Aggregators (PA), while the Insurance Regulatory and Development Authority of India (IRDAI) has published Information and Cyber Security Guidelines²⁵ for the insurance sector. Regulations related to cyber security are also encompassed under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016²⁶, and the Credit Information Companies (Regulation) Act, 2005²⁷.

Furthermore, financial authorities have specific rules and directives regarding the maintenance of financial transaction records and customer verification under the Prevention of Money Laundering Act, 2002²⁸ (PMLA). Authorities like SEBI, RBI, and IRDA have imposed obligations on securities market intermediaries and established guidelines on anti-money laundering and counter-financing of terrorism measures. These regulatory measures aim to ensure the security, privacy, and integrity of financial transactions and protect customers from potential risks in the fintech industry.

While challenges and areas for improvement remain, the regulatory measures implemented aim to strike a balance between promoting innovation and protecting customers. The evolving nature of the fintech industry and advancements in technology call for continuous updates and enhancements to the regulatory framework to address emerging risks and foster a secure and thriving fintech ecosystem in India.

²⁴ Payment and Settlements System Act, 2007, No. 51, Acts of Parliament, 2007 (India).

²⁵ Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security for insurers, IRDA/IT/GDL/MISC/ 082/04/2017, (Issued on April 7, 2017).

²⁶ The Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016, No. 47, Acts of Parliament, 2016 (India).

²⁷ The Credit Information Companies (Regulation) Act, 2005, No. 30, Acts of Parliament, 2005 (India).

²⁸ The Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).

V. ANALYSIS OF INTERNATIONAL JURISDICTIONS AND THEIR EXPERIENCE WITH FINTECH FRAUDS

Considering that India is the third-largest fintech ecosystem and is among the fastest-growing fintech markets in the world, the Indian fintech industry is envisioned to be valued at around USD 150 billion by 2025²⁹. Financial regulators not only in India but around the world recognize the need for innovation and work to support and promote FinTech activities by instituting regulatory virtual spaces because it can be challenging to integrate them into the current regulatory framework.

Not only is the growth of FinTech cybersecurity and fraud taking an upward turn, but new payment systems and instruments have also been found to be compromising the integrity of the market. Regulators must therefore strike the ideal balance between competitive advantages. Risks associated with integrating new technologies with current company models can be mitigated via fintech. As a result, financial services are one of the industries with the most regulation worldwide. Given that there are numerous financial ecosystems around the world, each with varying levels of complexity and regulatory systems, there is no one-size-fits-all solution that will satisfy all stakeholders in every state or work in every country.

Analysing international jurisdictions and their experiences with fintech fraud can provide insights into the challenges and measures taken to address fraudulent activities in the fintech sector. While it's important to note that the situation may vary across countries, here are some notable examples:

United States: The United States has seen several cases of fintech fraud, including Ponzi schemes, identity theft, and fraudulent investment schemes. Regulatory bodies like the Securities and Exchange Commission (SEC) and the Consumer Financial Protection Bureau (CFPB) have taken actions to combat fraud in the fintech industry. Enhanced regulations, such as Know Your Customer (KYC) requirements and anti-money laundering measures, have been implemented to mitigate risks.

United Kingdom: The UK has experienced various fintech fraud cases, such as payment fraud, phishing attacks, and crowdfunding scams. The Financial Conduct Authority (FCA) regulates fintech activities and has implemented measures to protect consumers and enhance

²⁹ The changing face of financial services: Growth of FinTech in India, Jun. 2022, <https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/publications/the-changing-face-of-financial-services-growth-of-fintech-in-india-v2.pdf>.

cybersecurity. The UK has also established the National Cyber Security Centre (NCSC) to address cyber threats and provide guidance to businesses, including fintech firms.

Singapore: Singapore has witnessed instances of fintech fraud, particularly in areas like peer-to-peer lending and investment scams. The Monetary Authority of Singapore (MAS) regulates fintech activities and has introduced stringent regulations, including robust licensing requirements, mandatory cybersecurity measures, and fraud detection frameworks. The MAS encourages collaborations between fintech companies and financial institutions to enhance fraud prevention measures.

Australia: Australia has faced fintech fraud challenges, including identity theft, fraudulent mobile banking apps, and online payment scams. The Australian Securities and Investments Commission (ASIC) oversees the fintech sector and has introduced measures to protect consumers. The ASIC focuses on ensuring compliance with financial regulations, promoting consumer education, and encouraging industry collaboration to combat fraud.

European Union (EU): The EU has encountered fintech fraud cases ranging from money laundering to data breaches. The European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) regulate fintech activities within the EU. The EU has introduced the General Data Protection Regulation (GDPR) to protect personal data and implemented anti-money laundering directives to combat financial crimes.

China: In contrast, some countries have less robust laws and regulations in place. For example, in China, there is no specific law that governs cyber security in transactions. Instead, companies are expected to abide by general laws and regulations. Such legislation requires companies to implement security measures to protect personal information and report data breaches to the government, but it does not have the same level of fines and penalties for non-compliance as GDPR. However, the region has seen a surge in FinTech frauds, particularly those involving mobile payments. For example, in 2018, China faced a major scam involving mobile payments where consumers were duped into transferring money to fraudsters.

Overall, it can be seen that laws and regulations for transaction-related cyber security vary greatly around the world. Some countries have specific laws and penalties for non-compliance, while others rely on general laws and regulations. Businesses operating internationally should be aware of the different laws and regulations in the countries where

they operate to ensure compliance and protect against cyberattacks and data breaches. Not just businesses, but there have been cases of mass cyberbullying done by one nation against another. Therefore, proper governance of cyber laws is necessary so that national interests are protected.

VI. CHALLENGES AND DRAWBACKS IN THE FACE OF TRANSITION TO A DIGITAL ENVIRONMENT

In spite of these laws, there are some inadequacies in India's implementation of data privacy measures. These challenges can hinder the effective protection of data privacy and the prosecution of cybercrime.

1. Lack of awareness and understanding: Many individuals and organisations are not familiar with their rights and responsibilities under data privacy laws. The IT sector has grown at such a rapid pace that it has become difficult for the masses to adapt to this fast-growing technology. *While the overall literacy rate in the country has to bridge a gap of 25- 30%, digital literacy is almost non-existent among more than 90% of India's population. At the same time, there has been a concerted push towards deeper penetration of the internet, along with the phenomenal increase in smartphone usage.*³⁰

This suggests that although there are more people using technology and the internet, they are still largely ignorant of the necessary safety and security precautions. This lack of awareness can discourage people from reporting incidents and hinder the effective development, comprehension, implementation, and compliance with data privacy regulations.

2. Insufficient technical know-how: Many businesses and government organisations lack the necessary resources, expertise, and training to effectively defend against cybersecurity threats. This deficiency in technical capabilities puts personal data at risk and undermines data privacy measures.

³⁰ Dilip Modi, *Fostering digital literacy in rural India*, ETBFSI, Sep. 25, 2022, <https://bfsi.economicstimes.indiatimes.com/blog/fostering-digital-literacy-in-rural-india/94402027>.

3. Lack of technical expertise among law enforcement agencies: One of the major challenges in India's cybercrime landscape is the lack of specialised knowledge and skills among law enforcement agencies. This deficiency hampers their ability to effectively investigate and prosecute cybercrime cases. As a result, there is a lack of accountability and deterrence for cybercriminals. It is crucial to provide comprehensive training and resources to law enforcement personnel to bridge this knowledge gap and enhance their capabilities in handling cybercrime. By doing so, the accountability of cybercriminals can be improved, leading to a stronger deterrent against cybercrime activities.

4. Coordination challenges: The lack of coordination among law enforcement agencies and government departments in India hinders the effective investigation and prosecution of cybercrime cases, particularly those that involve multiple jurisdictions. This coordination gap creates challenges in sharing information, collaborating, and allocating resources needed for successful investigations. As a result, it becomes challenging to gather evidence, apprehend cybercriminals, and ensure a swift legal process. Enhancing coordination mechanisms and establishing clear protocols for cross-jurisdictional cybercrime cases is crucial to overcome this hurdle and improve the efficiency of cybercrime investigations and prosecutions.

5. Outdated cyber laws: Existing cyber laws in India may lag behind the rapid pace of technological advancements and the ever-changing landscape of cybercrime. This creates difficulties in effectively prosecuting cybercriminals who use modern technologies. The Digital Personal Data Protection Bill of 2022 has faced criticism for certain provisions that privacy advocates argue could put personal data at risk due to their broad and ambiguous interpretation. Furthermore, Section 66A³¹ of the IT Act was struck down by the Supreme Court of India in the case of *Shreya Singhal v. Union of India*³² because it was deemed unconstitutional and violated the right to freedom of speech and expression. The court ruled that the provision allowed for arbitrary and excessive restrictions on online speech. Therefore, it is critical to upgrade existing laws to keep up with revolutions and the crimes that result from them.

³¹ Information Technology Act, 2000, § 66A, No. 21, Acts of Parliament, 2000 (India).

³² *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

6. Challenges in e-Governance Implementation: The National E-Governance Plan (NEGP) has faced significant challenges in its implementation, with many states struggling to provide the necessary infrastructure and resources. Although the Indian government is spending a lot of money on e-government projects, these projects are not successful in all parts of India. One of the main reasons for the same is the gap, or “digital divide”, that is prevailing in most parts of India. Not all regions in India are technologically equipped, which further raises the concern of an unequal distribution of ICT services.

7. Slow legal process: Insufficient workforce and subject-matter expertise within the legal system result in delays in the investigation and prosecution of cybercrime cases. These delays impede the accountability of cybercriminals and can discourage victims from reporting incidents. To tackle this issue, it is important to strengthen the legal and executive sectors by increasing the workforce and enhancing subject matter expertise.

Addressing these identified drawbacks and criticisms requires a collaborative effort involving the government, businesses, civil society, and law enforcement agencies. It entails raising awareness about data privacy rights and obligations, providing technical training and resources, improving coordination among relevant entities, updating cyber laws to align with technological advancements, bridging the digital divide, and enhancing the efficiency of the legal process. By addressing these inadequacies, India can better protect data privacy and effectively combat cybercrime.

VII. POLICY RECOMMENDATIONS

Traditionally, the world had only witnessed physical or corporeal frauds and scams, and it can be seen that the world lacked the regulations and expertise necessary to tackle the sudden changes that the digital revolution had brought with it. The legal ramifications surrounding the digital economy should not be the cause of an increase in cybercrime; instead, they must protect the privacy and trust of digital users worldwide.

To address these challenges and mitigate the risks associated with cybercrime, strong security measures, regularly updating software and systems, educating users about cybersecurity best practices, and fostering a culture of security awareness need to be implemented. Furthermore,

collaboration between different stakeholders is essential to combating cybercrime effectively and promoting responsible digital behavior.

The user's negligence or ignorance is the starting point for any digital crime. As a result, those in charge of the internet must always be aware of internet hunters and take precautionary measures. The need to educate citizens who are reluctant to adopt such technological revolutions about IT and digital apps cannot be overstated. As it is said, *"The best way to save yourself from a hacker is to hack yourself."*

In the modern world, where hardly any home is without a smart device, it is essential to inculcate, in the curriculums of educational institutions, the measures to tackle cybercrimes to instil a culture of responsible digital behaviour from an early age by conducting regular awareness drives targeting organizations, businesses, and even remote areas, promoting cybersecurity education, etc. in order to uplift technological literacy.

The Indian cybersecurity laws have been amended several times since the IT Act was first enacted in 2000. Amendments often create ambiguity and a lack of uniformity. To maintain widely recognised cybersecurity standards, India must enact more holistic and informative cybersecurity legislation, as well as clarify regulatory requirements and make policy changes to develop a better cybersecurity structure and data protection laws. Applying a similar methodology to cyber security laws as that of environmental laws, with specific and distinct rules for different aspects, can be a plausible approach. Just as environmental laws address distinct areas such as air, land, and water, cyber security laws can be tailored to various aspects of the digital realm.

It is crucial to strengthen cybercrime laws by reviewing and updating existing legislation to address emerging threats. This involves clearly defining cybercrimes and establishing appropriate penalties that reflect the severity of the offenses. Additionally, fostering international cooperation and extradition treaties can facilitate cross-border investigations and prosecutions of cyber criminals.

Enhancing law enforcement capabilities is another vital aspect of curbing cybercrime. This includes investing in training programs for law enforcement personnel, equipping specialized cybercrime units with the necessary tools and technologies, and fostering collaboration between law enforcement agencies and the private sector.

Public-private partnerships play a significant role in implementing cybersecurity policies and legislation. The Cybersecurity Information Sharing Act, 2015³³ (CISA) allows government agencies and private entities to share information about cyber threats and defensive measures³⁴. It aims to improve cybersecurity by facilitating information sharing across sectors and agencies. Governments should encourage collaboration between government agencies, private sector entities, and civil society organizations. By working together, they can develop coordinated strategies, share information and best practices, and undertake joint initiatives to strengthen cybersecurity measures across industries.

International cooperation is essential in the fight against cybercrimes, particularly in the case of transnational offenses. Governments should actively engage in international forums, such as INTERPOL and United Nations initiatives, to share intelligence, establish protocols for cooperation, and harmonise efforts to combat cyber threats globally.

It is all-important to create legislation that prevents financial fraud in light of advancements in the digital economic sector, such as blockchain technology and the growth of the e- investments market. Furthermore, better and more cost-effective online infrastructure for digital payment setups can be provided so that services are easily accessible to all segments of society. To deal with the globalised era of digitalization, it is critical for the Indian legal system to learn from its mistakes of the past and implement the recommendations that are feasible in approach. By examining the structures of digitally advanced economies, we can create better institutions for governance, offer a solid and stable system to an emerging nationlike India, and elevate the Indian fintech industry to a higher pedestal.

International jurisdictions have taken various approaches to tackle fintech fraud. To illustrate, key aspects of the GDPR include defining obligations for organizations to safeguard personal data and maintain privacy, granting individuals specific rights that can be legally enforced, and empowering regulators to demand proof of accountability and impose severe penalties for failure to comply. Additionally, it addresses jurisdictional conflicts that may arise when resolving international issues. As a result, continuous monitoring and adaptation to evolving fraud techniques are essential to ensuring the integrity and trustworthiness of the fintech ecosystem.

³³ Cybersecurity Information Sharing Act, 6 U.S.C § 754 (2015).

³⁴ The Federal Government of USA, Cyber Threat Indicators and Defensive Measures under the Cybersecurity Information Sharing Act of 2015, (Issued on February 16, 2016).

VIII. CONCLUSION

With its ability to conduct business without regard to national boundaries and its significant impact on every sector of society, the digital economy continues to spur advancement not only in India but also all over the world. Although there are laws and statutes governing online activities, it is imperative to ensure that these rules keep up with the latest industrial advancements. In the upcoming years, we are expected to witness a plethora of initiatives that will contribute to evolving cyber legal frameworks and related ecosystems in India. One of the required developments in Indian cyber law jurisprudence is the National Cyber Security Strategy. This strategy not only aims to build on the National Cyber Security Policy but also serves as a thorough guiding principle for people, decision-makers, and other stakeholders. The plan shall shed more light on appropriate response mechanisms concerning the enhancement of the public sector and other industries. To address jurisdictional challenges, international cooperation and collaboration are crucial. Countries strengthening their legal frameworks, enhancing capabilities for investigating and prosecuting cybercrimes, and establishing mechanisms for swift and effective information sharing will improve coordination and standardisation of laws, and international agreements can help overcome these challenges and facilitate the global fight against cybercrimes. Only by identifying gaps in the digital economy and implementing targeted digital solutions can a complex regulatory system be resolved. If artificial intelligence is employed to commit cybercrime, then it can also contribute to the development of a powerful digital force within the legal system. As a result, it is possible to conclude that India, as one of the top scorers in digital thrift, can also have solid legal structures, but only if legislation is enacted without any ambiguity or obfuscation to ensure the utmost protection of digital users' personal data.

RESERVE BANK OF INDIA'S CENTRAL BANK DIGITAL CURRENCY (CBDC)

-Anchal and Harsh Srivastava³⁵

I. INTRODUCTION

RBI in public domain has taken the decision to bring the central bank digital currency into the public domain. Digital rupee pilot project will be launching. Rbi has announced to launch Central bank Digital Currency (herein referred as CBDC) for the retail user. It makes sense for central banks to issue digital currency for widespread use a step after the creation of physical cash. But the argument over the only recently has the issuance of digital central money that is usable by regular users accelerated. At first, policy reports were issued with caution. The recent years have noticed the discussion expanding. The rise and fall of cryptocurrencies is accompanied by worldwide stable coin ideas, like Facebook's Diem, are emerging, and technological central banks have taken a more proactive position by predicting a day when there will be financial turmoil. The monetary system will have changed as a result of innovation instead of using the existing system as the standard. Central banks have started interacting in studies on CBDCs and, in certain cases, also in their creation. survey claims research on CBDCs is being done by 86% of central banks worldwide as of 2020, and 56 central Banks have disclosed their efforts at research or development in the public sphere (see Boar and Wehrli (2021) likewise Auer et al. (2020). Two central banks have established CBDCs as of these writing, and numerous others are in carrying out tests. However, central banks have not yet reached a consensus on the necessity of issuance of CBDC.

As it is being said right now, CBDCs are a type of digital currency that is valued in the group of central banks (2020). These can be used either for retail use (i.e., by households and businesses) or wholesale use (i.e., by financial institutions businesses - the public at large). They are token-based, a kind of identity, that allows for payment anonymity. A CBDC can be founded on either traditional technological infrastructures or distributed ledger technology (DLT). In the majority of cases, CBDCs are being created so that the two-tier monetary system is preserved system with a labour distribution that divides the public and commercial sectors. It is a digital form of the paper currency. It will be a legal tender which will be issued and backed by the RBI. RBI will have control over it and therefore RBI will be the regulator of the paper currency. Therefore, this CBDC will have some authenticity and

³⁵ The Author are students in their 2nd year and 4th year at the CHANAKYA NATIONAL LAW UNIVERSITY.

accountability to the people. This type of currency is exchangeable with the Fiat currency. It is said that in the starting only selected locations like bank will be taken into consideration. Also participating customers and merchants are also included in the pilot project of the scheme. In the 1st phase only 4 cities i.e Mumbai, Bengaluru, New-Delhi and Bhubneshwar will be taken into consideration. It will be generated in the form of the token which will represent the legal tender. And this token will be issued in the same denominations as paper currency or the coin. For exp. If a person has 100 rs in the form of paper currency or in the form of coin then in same way this e-rupee will be generated. This will be distributed through the intermediaries i.e. bank. It will empower the users to transit with rupees with the digital wallet which will be offered by the bank. Later on it will go in the devices of the users. Therefore, it will empower the user to transfer from person to person or the person to the merchant at the pilot level. Payment can be done by the QR codes. Therefore it is also considered that it will take over the UPI system. IDFC, ICIC Yes Bank and SBI will be the 1st four bank who will be implementing this scheme.

1. Purpose

It is considered that e rupee will be the electronic version of the cash and therefore it is considered that it is meant for the retail transactions (people to people transactions are possible through this plan).

2. Safe Money

Payment settlement record of every transaction will be available therefore no black money will be circulated in the economy

II. HISTORICAL BACKGROUND OF CBDC AND IMPLEMENTATION IN REAL WORLD

A The digitalization of money is turning point. Technology progress in money like the Bahamian sand dollar, stable coins like the libra/diem, and virtual (crypto) currencies like bitcoin. These financial and monetary advances echo earlier changes in monetary history: 1) The transition from commodity money (gold and silver coins) in the eighteenth and nineteenth centuries to fiat money 2) The transition from central bank notes to a central bank monopoly in the nineteenth and twentieth centuries

To fulfil the evolving economic needs, several types of money have emerged throughout history. Credit cards, checks, banknotes, and coins were all advances in their respective eras (Giannini, 2011). New payment technologies, including stablecoins and CBDCs, a new type of central bank-issued currency.

The existing types of central bank money, can be thought of as analogous to CBDCs in a digital sense. Wholesale CBDCs have the potential to develop into a new method of settlement CBDCs would be a liability for the central bank and a form of "digital cash" that anybody may use. It's not a novel concept to provide access to digital money. Tobin (1987), for example, suggested the use of "deposited currency," or "a medium combining the ease of deposits and the safety of money," to improve payments and lessen the need for deposit.

Several central banks have launched internal initiatives over the past few years to better comprehend cryptocurrency technology. These largely came to the conclusion that DLT wasn't yet developed enough so that it can be used.

Several central banks began conducting research on digital currencies in 2016 for commercial purposes. Many of them concentrated on using DLT to settle high-value interbank payments.

Some entailed central bank collaboration on wholesale CBDCs for international payments.

Sweden's Riksbank published the first research on retail CBDC 2017. This paper evolved "e-krona" project.

The public, as well as international tourists visiting China, will be able to access the PBC's e-CNY through account-based interfaces. Meanwhile, the Sand Dollar, widely regarded as the first live retail CBDC, was released by the Central Bank of the Bahamas in October 2020. In March 2021, (ECCB) debuted DCash. People-to-people (P2P) transactions and financial transactions between customers and merchants are both possible with DCash, which is supplied by authorised financial institutions.

In Graph 2 Overall, it is evident that central banks have been working on CBDCs since at least the middle of the 2010s and that this work will continue into the 2020s. At least three nations—Ukraine, Uruguay, and Ecuador—have finished a retail CBDC trial. There are eight active retail CBDC pilot projects, some of which are in Sweden, China, and Korea. In the meantime, 19 central banks and 40 central banks have published research on retail CBDCs.

III. MONETARY TRANSACTIONS IN HISTORY

History's monetary changes have been fueled by evolving technology, shifting consumer preferences, economic expansion, and the need to properly fulfil the duties of money. The evolution of money (and finance) throughout human history (Goetzmann 2017). The current digital shift was made possible by three historical developments.

1. Fiduciary money (convertible bank notes) was first introduced in the 18th and 19th centuries as a result of new financial technology, which significantly decreased the resource costs of specie (Smith 1776). Furthermore, in the early modern age, governments *issued inconvertible fiat currency* due to the pressures of rising war finance expenditures. The next stage in this development seems promising for CBDC as a social alternative to fiat money.
2. It has been argued for government control of commercial banking and for a government monopoly on note issuance based on the historical record of poorly regulated private banks issuing notes that were allegedly convertible into coin (Friedman 1960). The US's history of free banking has been marked by significant turbulence (Gorton 1986). The central bank/government monopoly finally became the dominant force in the note market. The current growth of stablecoins and cryptocurrencies indicates that a process of consolidation toward CBDC may potentially be the end result.
3. From the 17th to the 20th centuries, central banks developed to meet various significant societal demands, including war financing, an effective payments system, financial stability, price stability, and macroeconomic stability. Monetary policy has developed into the flexible inflation targeting that it is today based on credibility for low inflation through a gradual and costly learning process. CBDC might continue this practise.

IV. APPLICATION OF CBDC IN REAL WORLD

The introduction of CBDC raises several significant issues with regard to its conception, which central banks have carefully considered. The decision between wholesale and retail CBDC is one difficulty. The wholesale payments clearing mechanism has seen significant changes, which suggests that the retail CBDC is the main problem. Here, the part of currency that serves the public good offers a compelling case for either direct distribution or at the very least stringent control and oversight by the government. The private sector has a competitive

edge in financial innovation, but accounts at the central bank are certainly viable. Consequently, a two-tiered or public-private model may be preferred in advanced nations. The general public might be offered CBDC accounts by designated institutions, or they might act as channels for the central bank (Tobin 1987).³⁶The second issue is the worry of well-known authorities. According to research, central banks' balance sheet policies, restrictions on CBDC ownership, or tiering of interest rates for accounts with and without CBDCs might all counteract disintermediation are sufficient lines of defence for central banks against runs.³⁷

V. REQUIREMENT OF DIGITAL CURRENCY DURING COVID-19

It was held that during the pandemic market started shifting to the digital world. Market shattering hopes that the "digital gold" Bitcoin would provide a safe refuge in times of economic and social unrest. MakerDAO, one of the most important DeFi (Decentralized Finance) platforms, learned the hard way that its decentralised lending protocol did not work as expected in tumultuous times. Emergency governance measures were rapidly enacted, but the damage and loss of part of the confidence had already occurred. Maker was accused of failing to adequately disclose dangers in a class-action lawsuit brought by one of its customers in the US. Despite the pandemic, not all was hopeless for the crypto and blockchain world.

A trend away from cash to digital payments had been driven by concern of COVID-19 spreading through bank notes and coins. This concern had also rekindled interest in digital assets and encouraged discussions of central bank digital currencies (CBDC). The fact that China's much awaited CBDC, followed quickly by an updated proposal for the Facebook-backed Libra, suggested that these events were not just coincidence (one supposed to overcome staunch opposition from governments worldwide). In addition to the Dutch Central Bank publishing its own CBDC-related thoughts, France called for CBDC tests. Although there were numerous worries regarding privacy public stablecoin projects were competing for a first-mover advantage.

³⁶ Andolfatto, D (2021), "Assessing the Impact of Central Bank Digital Currency on private banks", *Economic Journal* 131: 525-540.

³⁷ Auer, R and R Bohme (2020), "CBDC Architectures, The Financial System, and the Central bank of the Future", VoxEU.org, 29 October.

CBDC had drawn greater attention, but not solely because of concern over coronavirus transmission. Following the COVID-19 outbreak, numerous nations had quickly authorised emergency aid for individuals, families, and companies. However, issues had plagued the delivery of those money. For instance, the US government relied on conventional banks to authorise commercial funding. Banks had been charged with diverting emergency money to their chosen clients (including private equity-backed enterprises) rather than to small businesses who were most in need because they got a (very large) 1-5% fee for each loan issued.

The transfer of public monies to people who need them most has been praised as a benefit of CBDC and other digital assets. There have been ideas for "retail" CBDC; each of us might have an account with our central bank, and when we needed it, it would deposit CBDC right into our online account. Our central banks would automatically deposit emergency money into our personal or business digital "wallets," eliminating the need for us to wait for regular commercial banks to approve paperwork for such funding. Such proposals have unique difficulties (such as the broader impact on commercial banking, hacking and surveillance concerns). Because these tools are new and unproven, we will need to give considerable thought to their design. If properly developed, they might, nevertheless, improve trust and openness in difficult circumstances.

The first significant wave after demonetization was noticed to be the widespread acceptance of digital payments. The second significant wave for digital payments emerged during the pandemic and lockdown. In India, where three out of every four consumer purchases are made in cash, the central government has long attempted to promote digital payments. The Central Government in November 2016 with the aim of reducing inflation, which, as he also remarked, later assisted in promoting a move toward digital transactions. In the contemporary environment of social distance, the government introduced India Pay Safe through our ongoing "UPI chalega" programme to spread awareness. It was hoped that many people who were accustomed to handling money would be inspired by it.

These services are useful for

- Transfer
- from one person to a business (such as kirana stores),
- from one business to another (like a retailer to a supplier), and
- from one business to another (such as reimbursements, and claims), and
- from one business to another.

VI. OUTCOME OF THE STUDY REPORT

However, India is seeing an increase in digital payments. This year, digital purchases in the nation of over 1.5 billion people reached a new high, as they have in most other parts of the world. The local outlet reported for the first time that there was dramatic increase across all channels, from the universal payment interface (UPI) to the Aadhar-Enabled Payment System (AEPS). Digital payments and fintech hit historic highs in 2020, despite the fact that the Covid-19 outbreak and the economic lockdown caused a large number of individuals to stay at home and maintain social distances. Many people started using their smartphones to make purchases and even take loans for smooth banking services due to concerns that visiting bank branches and using currency notes could spread new coronavirus infections. This development occurred not just in metro areas but also in smaller communities. As a result of the COVID-19 lockout and its associated restrictions, an enormous 126 percent increase in digital transactions was recorded in Uttar Pradesh in 2020 as compared to 2019. At the point of sale of terminals in stores, the Card spends between 60 and 70 percent of the average in January. This indicates that individuals use digital payments for real-world activities like shopping. All platforms, including the Unified Payments App and the (AePS), had a record-breaking increase in digital payments in 2020.

PAYMENT TRANSACTION IN THE YEAR 2020

No. of
Transaction

(in Crore)

Growth

in %

(month

on

month)

Jan 2020 436.43

Feb 2020 847.44 94.17

March 2020 1,262.84 49.02

April 2020 1,566.22 24.02

May 2020 1890.23 20.69

June 2020 2,298.85 21.62

July 2020 2,699.06 17.41

August

2020

3,132.43 16.06

	Transactions in crore	Growth in % on the monthly basis
Jan 2020	436.43	
Feb 2020	847.44	94.17
March 2020	1262.84	49.02
April 2020	1566.22	24.02
May 2020	1890.23	20.69
June 2020	2298.85	21.64
July 2020	2699.06	17.41
August 2020	3132.43	16.06

Sep.2020	3620.51	15.58
October 2020	4108.29	13.47
November 2020	4623.25	12.53
December 2020	4764.28	03.05

No. of
Transaction
(in Crore)

Growth

in %

(month

on

month)

Jan 2020 436.43

Feb 2020 847.44 94.17

March 2020 1,262.84 49.02

April 2020 1,566.22 24.02

May 2020 1890.23 20.69

June 2020 2,298.85 21.62

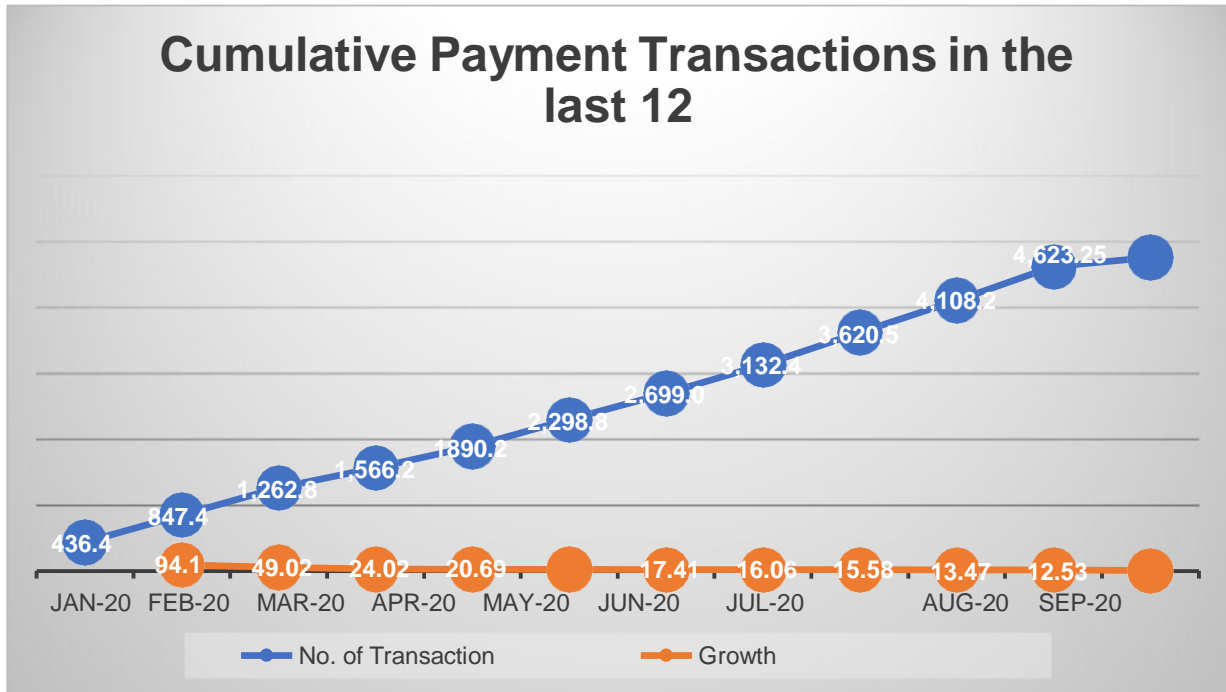
July 2020 2,699.06 17.41

August

2020

3,132.43 16.06

(Source: digipay.gov.in)



UPI transactions reached a new high of 221 crore transactions worth 3.9 lakh crore in November after surpassing the 200 crore threshold in October. Players were optimistic that the Center's objective of \$4,630 billion for digital payments in 2020–21 will be surpassed. Even though demonetization was the catalyst for India's 2016 initial launch of digital payments, the government's actions remained convoluted over time. According to Manish Patel, founder and CEO of Mswipe, the global pandemic sped up and broadened India's adoption of digital payments and trade.

In December 2020, contactless payments accounted for 30% of all transactions at Mswipe, up from 13% in January 2020.

VII. STATUS OF CRYPTOCURRENCY DURING COVID-19

In the recent article, an empirical investigation was performed to see if the Covid-19 pandemic epidemic impacted the cryptocurrency market (often known as the "cryptomarket")³⁸. After a year of the pandemic, this market seemed to have taken off. For instance, Bitcoin, the first cryptocurrency in the world, could be bought for around \$7,300 at the time the epidemic broke out. The same token now costs more than \$46,800, a startling increase of 640 percent. Similar (or even higher) rises were also seen in other prominent cryptocurrencies, such as Ether. One set of factors could result in increased demand for cryptocurrencies in the event of a pandemic. Cryptocurrencies may be exchanged from anywhere in the world, which somewhat reduces the possibility of liquidity problems if local governments prohibit trading as part of a lockdown. As a result, cryptocurrency gained appeal over competing options. Investors may also want to migrate their investments to the decentralised cryptomarket if they are concerned that a crisis would lead to market intervention from central banks or other political actors. In other words, because cryptocurrencies run automatically rather than under the control of a single institution, they could help investors reduce some of the political risk, making them more desirable.

VIII. HOW IT WILL REPLACE UPI

CBDC will never take place of UPI but enforcement of CBDC will certainly enhance its applicability. "General purpose CBDC, also known as retail CBDC, and wholesale CBDC are two categories for CBDC. The wholesale CBDC was created by the RBI to settle interbank transfers and related activities. The wholesale CBDC can greatly improve the security and efficiency of the transaction settlement systems. Additionally, this will strengthen the nation's entire digital economy and promote greater financial inclusion.

³⁸ Hadar Y. Jabotinsky and Roe Sarel, The CLS Blue Sky Blog, March 26, 2021

IX. HOW CENTRAL BANK DIGITAL CURRENCY DIFFERENT FROM UPI

- As with other digital payment methods like UPI, IMPS, debit or credit card transactions, etc., the digital rupee or it will be the primary payment method utilised for digital transactions in place of money or cash. The digital rupee, or CBDC, is a legal tender in and of itself and need not be backed by actual currency, in contrast to UPI transactions which are fully backed by physical money.
- Simply put, UPI is an interface for financial transactions that take place between two bank accounts, an account and a digital wallet, or a digital wallet and an account. The Digital Rupee, on the other hand, is just one more kind of money that is similar to fiat money.
- Similar to cash, CBDC can permit the direct transfer of funds between two private persons, businesses, or other organisations. While just two bank accounts can be moved while using UPI.
- Unlike CBDC, digital payments conducted through UPI and IMPS must be supported by physical money or be settled by the transacting banks with the central bank in order for each rupee to be transferred. The benefit of using digital money over UPI, where each bank has a different UPI handler, is that transactions will be resolved promptly because they are handled by clearing houses that have direct backing from the central bank.
- CBDC is more effective since it avoids the intermediate step of connecting bank accounts with online payment systems, but it also gives the government more visibility into real-time transactions.

Their utility will vary, but they will coexist. CBDCs can function as digital banknotes in the upcoming digital economies because the world is shifting toward being more digital than physical. Experts predict that the Central Bank Digital Currency (CBDC), which was recently launched, would coexist rather than compete with the Unified Payments Interface (UPI).

"Digital currency accounts won't ever entirely replace the actual bank with savings accounts. The adoption of digital currency may be hampered by the fact that accounts will be in the form of digital wallets. Instead of competing with UPI, the CBDC will coexist with it "Director and COO of Livfin Pooja Sondhi remarked. The digital rupee is now less practical than UPI because it has only been made available to a limited number of users in a closed- user group (CUG). The digital rupee is like currency and won't leave an audit trail, whereas UPI is a bank-to-bank transfer where banks know who you are paying and how much. And since the applications for CBDCs and UPI differ, and one cannot take the place of the other.

X. ADVANTAGES AND DISADVANTAGES

The digital rupee could assist address the growing need for digital currencies, which is evident from the emergence of private digital currencies like bitcoin and the expanding use of digital payments.

The significance of CBDCs:

- **More dependable than private digital currencies:** It is noteworthy that central bank digital currencies may be a trustworthy, government-backed substitute for private currencies, which are frequently unstable and unregulated.
- **Low or insignificant cost of creating digital currency:** The electronic creation and distribution of the digital rupee virtually removes the cost of printing and distributing physical currency.
- **Greater control over monetary and fiscal policy:** CBDCs can make it easier to conduct monetary and fiscal policy because it not not like physical currency untraceable.
- **Promote financial inclusion:** By integrating the unbanked into the financial system, CBDCs can also aid in the economic promotion of financial inclusion.
- **Boost to Digital Economy:** The digital rupee will provide the Indian digital economy a "huge boost" and enable India to take use of the system's advantages.

XI. CONCERNS/CHALLENGES RELATED TO CBDCS:

- **Financial Stability:** CBDCs can potentially impact financial stability in the following ways:
- **Systemic Risk:** CBDCs can enhance the resilience of the financial system by reducing systemic risk. With CBDCs, central banks can have real-time visibility into transactions, enabling them to monitor and respond to risks more effectively. Additionally, CBDCs can minimize counterparty risk by providing a risk-free digital asset.
- **Bank Deposits and Liquidity:** CBDCs may lead to changes in the behavior of depositors. If individuals and businesses start to prefer holding CBDCs instead of traditional bank deposits, it could impact banks' ability to provide loans and manage liquidity. This shift in deposit behavior could have implications for monetary policy implementation and the stability of commercial banks.
- **Financial Intermediation:** CBDCs could potentially disrupt the traditional role of commercial banks as intermediaries between savers and borrowers. Direct access to CBDCs by individuals and businesses might reduce the need for traditional bank accounts, affecting

banks' ability to lend and earn interest income, thus altering the dynamics of credit creation and monetary policy transmission.

- **Impact on credit creation:** As digital currencies gain popularity, people can start taking money out of their bank accounts. The quantity of loans that the banks produce may be impacted by the significant capital flight from bank accounts to digital currencies.
- **Privacy worries:** The centralised nature and traceability of the currency that will be used digitally raises the concerns related to the privacy as the transactions will be regulated digitally and all the transactions related data can be manipulated thereof. **Transaction Surveillance:** CBDCs can provide central banks with granular transaction data in real-time, enabling extensive surveillance. While this can help combat illicit activities, it also raises concerns about privacy invasion. The extent of transaction monitoring and data retention policies would determine the balance between privacy and regulatory objectives.
- **Centralization of Data:** CBDCs centralize financial data with the central bank, potentially creating a single point of failure and making the system vulnerable to cyberattacks or data breaches. Adequate measures would need to be implemented to safeguard user data and prevent unauthorized access or misuse.
- **Anonymity and Pseudonymity:** Design choices regarding the anonymity or pseudonymity of CBDC transactions will be crucial. While complete anonymity could facilitate illicit activities, too much surveillance may erode privacy. Striking the right balance is essential to maintain privacy while addressing regulatory concerns. **Financial Exclusion:** Privacy concerns might discourage individuals from using CBDCs, particularly if they fear their financial data could be misused or exposed. This could potentially widen the digital divide and exclude certain populations from participating in the financial system.
- **Incapability to supplant private digital currencies:** People who have lost faith in fiat currency issued by central banks are the main group driving demand for private currencies. The demand for private currencies is unlikely to be impacted by the mere digitalization of a national currency like the rupee. One of the main factors contributing to the popularity of private digital currencies is the demand for anonymity. The appeal of digital currencies produced by central banks may be impacted by the lack of privacy.

XII. ISSUING OF CBDC WITH CONCERNED PRINCIPLES

The moment is right for CBDCs as a concept. If correctly created, they offer a chance to enhance payments through a modernised version of central bank. They might by permitting widespread access, they serve as the framework for a brand-new, highly effective digital payment system. They may also contribute to robust data governance and privacy requirements.

However, more research on CBDC design decisions and their implications is required to get financial stability. According to Adam Smith, money has three basic functions in society: it serves as the benchmark for economic activity; a store of value for the gradual transfer of purchasing power. The basic objective of CBDCs is to offer a common medium of exchange for the digital economy. By providing a global store of value, they do not, however, want to dis-intermediate the banking industry.

Research in this area is assisting in understanding how to maximise the usefulness of CBDCs as a payment method while minimising the overall inflows to central bank balance sheets. Further research is still needed on a number of significant and complex issues, such as the interoperability of new and existing infrastructures the effects of CBDCs on international trade.

Researchers will need to work through the details of cross-border. As a result, more research is needed to complete the examination of interoperability with non-CBDC payment options. For CBDCs to be properly designed as a new form of money in the digital age, the answers to these open questions will be essential.³⁹

XIII. RECOMMENDATIONS

The following steps could be implemented to alleviate any potential drawbacks of the adoption of digital currency issued by central banks.

- The amount of money that a person can hold in the form of CBDCs may be capped by the central banks.

³⁹ Kahn, C, F Rivadeneyra and R Wong (2018): “Should the central bank issue e-money?”, Bank of Canada Staff Working Paper, 2018-58, December.

- Central banks may need to infuse new funds into banks to guarantee that depositors' rush to digital currencies does not impair banks' capacity to issue loans, which would assist prevent the widespread outflow of deposits from banks.

XIV. GLOBAL CBDC DEVELOPMENTS:

- CBDCs are now at various phases of development worldwide.
- The Bahamas introduced the first CBDC in the world in 2020.
- Several nations, notably those in the European Union, China, and the United States, have been attempting to issue their own Central Bank Digital Currency (CBDC) in recent years.
- Notably, some nations have abandoned plans to implement digital currencies due to concerns about the effectiveness of central bank digital currencies, notably Finland and Denmark.

XV. CONCLUSION

The moment is right for CBDCs as a concept. If correctly created, they offer a chance to enhance payments through a modernised version of central bank money that maintains the essential qualities of finality that any bank can offer. They might by permitting widespread access, they serve as the framework for a brand-new, highly effective digital payment system. They may also contribute to robust data governance and privacy requirements.

Be that as it may, more examination on CBDC plan choices and their large-scale monetary ramifications is expected to achieve the likely advantages for the public government assistance while keeping up with monetary steadiness and public-private area coordinated effort. As per Adam Smith, cash has three fundamental capabilities in the public eye: it fills in as a unit of record, the benchmark for monetary movement; a method for trade for installments; and a store of significant worth for the steady exchange of buying power. The essential goal of CBDCs is to offer a typical mechanism of trade for the computerized economy. By giving a worldwide store of significant worth, they don't, be that as it may, need to disintermediate the financial business.

Research in this area is assisting in understanding how to maximise the usefulness of CBDCs as a payment method while minimising the overall inflows to central bank balance sheets. Further research is still needed on a number of significant and complex issues, such as the

interoperability of new and existing infrastructures, access to and control of central bank funds, and particularly the effects of CBDCs on international trade.

Researchers will need to work through the details complete the examination of interoperability with non-CBDC payment options.

FANTASY SPORTS AND ONLINE GAMBLING: A VIEW THROUGH LEGAL LENS

- Ravi Ranjan and Rohit Sahay¹

ABSTRACT

Fantasy sports apps in India have seen a huge rise in the number of users over the past few years. According to Klynveld Peat Marwick Goerdeler (KPMG), India, the fantasy sports market might bring in more than 100 billion Indian Rupees (INR) in foreign direct investment over the following several years and generate over 1.5 billion online transactions by 2023.

In this article, the authors have aimed to analyse the legality of online gambling in India by understanding its status in India. The authors in this article talks about how fantasy sports are different from online gambling and what is the view of the courts regarding both of them. This article also intends to discuss the debate of 'chance v. skill' in light of the legality of fantasy sports. Further, to understand this, various case laws have been discussed. Further, this article also discusses the possible measures that can be taken for better regulation of fantasy sports in the Indian diaspora.

Keywords: Fantasy sports, Online Gambling, Chance, Skill, Regulation.

¹ Authors are in their 3rd year, studying at National University of Study and Research in Law, Ranchi.

I. INTRODUCTION

In India, more than 500 million people are linked to each other on a daily basis due to advances in mobile technology.⁴⁰ The internet has provided Indians with access to a variety of online platforms and services that were previously unavailable, and online gaming is one of the foremost industries to benefit from this.

In line with a report released by the Federation of Indian Fantasy Sports (FIFS) and Deloitte India, India is the largest fantasy sports market in the world, with over 13 crore users. The fantasy sports market in India is expected to increase by 38 percent CAGR from Rs 34,600 crore in Fiscal Year 21 to an estimated Rs 1,65,000 crore in Fiscal Year 25.⁴¹

The rise in online gaming has also exacerbated the hike in online gambling activities in India. Many Fantasy gaming apps like *Teen Patti* and *Dream 11* base their business model on online gambling or betting. A fantasy sport is a game that is played over several rounds (i.e., a single match, or an entire league). Participants form virtual teams by selecting players and acting as managers for their virtual teams. These virtual teams contest against one another for points based on the outcome or accomplishments of real athletes or teams competing in professional sports matches. The participant whose virtual team earns the most points over the course of the rounds is the winner. Fantasy sports have acquired relevance, as they give sports lovers the opportunity to play virtually and make them learn about the nuances and strategies of sports.

Fantasy sports claim that you could win lakhs of rupees in an instant on their platform. However, this method of making quick cash seems to be similar to gambling. It has all the characteristics, too — an entrance fee, large payouts, and betting on real-life players competing in competitive games. However, fantasy sports are legal by virtue of many judgments of the Supreme Court and High Courts. This paper will analyse the logic behind its legality and the need for uniform legislation to limit the legislative ambiguities related to online gambling and fantasy games.

⁴⁰ Nandita Mathur, *India now has over 500 million active Internet users: IAMAI, LIVEMINT* (May 5, 2020, 05:48 PM), <https://www.livemint.com/news/india/india-now-has-over-500-million-active-internet-users-iamai-11588679804774.html>.

⁴¹ Maryam Farooqui, *India becomes world's biggest fantasy sports market with 13 crore users: Report*, money control (Jan. 18, 2023, 11:04 PM), *India becomes world's biggest fantasy sports market with 13 crore users: Report*.

II. WHAT IS ONLINE GAMBLING?

According to the Black's Law dictionary, to gamble means *"to play, or game, for money or other stake; hence to stake money or other thing of value on an uncertain event. It involves, not only chance, but a hope of gaining something beyond the amount played."* Therefore, in other words, gambling (also described as betting) is the wagering of money or other valuables (referred to as "the stakes") on an unknown result with the prime goal of earning money or material goods.

Any form or type of gambling that takes place over the internet is known as online gambling or internet gambling. Casinos, digital poker, and sports betting are all examples of this. Many countries have restrictions or prohibitions on online gaming. It is, however, legal in many states of the United States, many regions of Canada, the majority of European Union memberstates, and many Caribbean nations.⁴²

III. STATUS OF ONLINE GAMBLING IN INDIA

In its latest policy change, Google allowed apps related to betting or gambling on its Play store in 15 countries, including Canada, the USA, and Australia. However, the new policy will not apply to India, as India is not on the list of countries where apps related to gambling are permitted. The explanation for this, according to reports, is that state governments have issued directives outrightly banning such apps. Paytm and Paytm First Games, for example, for allegedly allowing sports betting and daily fantasy sports, were recently temporarily barred from the Google Play store, as they violated Google's terms of service.⁴³ As a consequence, the App Store interface prevents the installation of several gambling applications.

⁴² Alan Draper, *Countries Where Online Gambling is Legal*, THE SPORTS DAILY (Dec. 23, 2022, 10:42 PM), <https://thesportsdaily.com/news/countries-where-online-gambling-is-legal/>.

⁴³ Jagmeet Singh, *Google Play Allows Gambling, Betting Apps in 15 New Countries Including US, Canada, and Australia*, GADGETS. NDTV (Dec. 23, 2022, 11:09 PM), <https://gadgets.ndtv.com/apps/news/google-play-gambling-betting-apps-policies-update-15-more-countries-us-canada-2359919>.

IV. HOW ARE FANTASY SPORTS DIFFERENT FROM BETTING

The main reason for the gaining popularity of fantasy sports is that it gives the players a chance to test their knowledge about the game. When a player predicts a good team, they feel great about their judgement and it makes them believe that they have a good understanding about the game which makes them feel proud.⁴⁴ Fantasy sports is very much different from betting as the result in betting is solely based on luck unlike fantasy sports where there is a need for skill to win. Fantasy sports can be regulated by the government unlike betting. In India, Federation of Indian Fantasy Sports (FIFS) is one such body which is devoted to work for best practices in online fantasy sports. Betting can be done by any person but in fantasy sports a person needs to submit details like bank account number, pan card, KYC details by which it can be ascertained that the person playing such games is eligible for it or not. Moreover, Fantasy sports is very much transparent as compared to Betting as in fantasy sport the players can check the team made by their opponents and there isn't any chance for fraud and also the payment is done through online certified gateways and hence eliminates the chance for illegal transactions.

V. LEGISLATIVE AMBIGUITY REGARDING FANTASY SPORTS

India's gambling laws are complex. There is absence of pan-India law for betting and gambling as the same comes under the State List as Entry 34. (i.e., List II of the Seventh Schedule).⁴⁵ This ensures that only the state legislature has the authority to enact betting and gaming legislation. Therefore, each state now has its own gambling act. Though Fantasy sports is not specifically mentioned under seventh schedule but till date it is kept under the ambit of gambling. As per Public Gambling Act, 1867 it was clearly mentioned that games involving skills will not come under the ambit of the act.⁴⁶ The 276th Law commission report was also of similar view and it held that a game involving skill should not be considered as gambling.⁴⁷ The commission wanted the legislature to interfere in the issue rather than outrightly banning it. Even Niti Aayog in its December 2020 report has talked about the lack

⁴⁴ EM Buzz, *here's why fantasy sport is different from betting*, EAST MOJO (Jan. 18, 2023, 11:21 PM) <https://www.eastmojo.com/sports/2022/04/19/heres-why-fantasy-sport-is-different-from-betting/>.

⁴⁵ The Constitution of India, 1950, Schedule VII, List II, State List, Item 22 (Betting and gambling).

⁴⁶ Public Gambling Act, 1867, § 12, No. 3, Acts of Parliament, 1867, (India).

⁴⁷ Law Commission of India, Report No. 276 on Legal Framework: Gambling and Sports Betting Including in Cricket in India, (July 2018).

of clarity regarding legislation of fantasy sports in India and how the ambiguity is affecting the growth of the industry. It also emphasised on various judgements given by the Indian courts in favour of deciding the legal status of fantasy sports in India.⁴⁸

When we look at the terms of conditions of Dream11, a fantasy sports app, it does not allow the residents from Nagaland, Sikkim, Assam, Andhra Pradesh, Telangana and Odisha to play any contest on its platform.⁴⁹ The reason for this is that the legislation of these states proclaims that a game which is a mixture of chance and skill cannot be played for money but all other states have a different legislation which does not impose such restrictions.

VI. FANTASY SPORTS AND ONLINE GAMBLING IN THE COURTS OF LAW

As the definition indicates, gambling refers to any activity in which a fee is charged in exchange for a chance to win a prize. For an action to be termed as gambling, the deciding factor for the victory of a person should be his luck and not his skill or knowledge. Courts in the USA commonly use some tests to determine whether the degree of skill required in influencing the outcome of a game is adequate to avoid violating a state's gambling laws. The *Dominant Factor test* examines if the game's result is influenced more by the contestants' skill than by luck. Similarly, in *Material Element test* and *Any Chance test*, it barely matters whether skill is a major, or even decisive, factor in the outcome of the game. If chance influences the game, it will be considered gambling.⁵⁰ In other words, to categorise a game as gambling, it should be a 'game of chance' rather than a 'game of skill.' A 'game of chance' is any game in which there is nothing a person can do to win, i.e., his knowledge or skills cannot help him reach the top. Instead, all he needs is a stroke of good luck to be the best player. In contrast, a 'game of skill' can be any game where a person's skill is of utmost importance, and the result of the game depends upon his expertise rather than his fortune.

Besides the 'game of skill' and 'game of chance,' there are some games in which luck along with skill play a vital role. In these games, the knowledge, experience, and ability of a person

⁴⁸ Niti Aayog, Report on Guiding Principles for the Uniform National- Level Regulation of Online Fantasy Sports Platforms in India, (Dec. 2020).

⁴⁹ C.C. Chengappa, *Which states have banned Dream11 in India?* THE BRIDGE (Apr. 15, 2022, 12:13 PM), <https://thebridge.in/esports/dream-eleven-states-banned-india-fantasy-sport-25922>.

⁵⁰ Neil Braslow, *A Legal Guide to Skill Gaming*, Braslowlegal.Com (Jul. 15, 2020), <https://braslowlegal.com/blog/2020/7/15/a-legal-guide-to-skill-gaming>.

are indispensable, accompanied by luck. The above tests play a major role in determining the legality of such games.

Like the Courts in the USA, the Indian Judiciary too, devised certain tests. In *State of Andhra Pradesh v. K. Satyanarayana & Or.*,⁵¹ The Supreme Court established the "preponderance of skill" test to determine whether a game is based on skill or chance. It was held that the game of Rummy involves preponderance of skill rather than chance as Rummy needs an unquestionable amount of skill when played. Memorisation is required for the fall of the cards and the building up of Rummy needs considerable skill in holding and/or discarding the cards.

A constitutional bench of the Supreme Court in *Dr. KR Lakshmanan v. State of Tamil Nadu & Anr.*⁵² held that for a game to be termed as gambling, the luck factor should predominate the skills. However, it should not be considered gambling if there is some element of luck, but the game is principally a game of skill. In another case, *State of Bombay v R.M.D Chamarbaugwala*⁵³, the test of preponderance was used by the Supreme Court to interpret the words 'mere skill.' The test of preponderance determines whether a game is based more on skill or on chance. The Court, in its judgment, stated that games of skill are primarily games of ability or adeptness. "A competition in order to avoid the stigma of gambling must depend to a substantial degree upon the exercise of skill," the Court opined.

VII. LEGALITY OF FANTASY SPORTS – CHANCE OR SKILL

To determine whether fantasy games should come under the ambit of gambling, firstly, we need to decide whether or not it falls under the category of "game of chance" or "game of skill." The Niti Aayog in its report emphasised that there isn't any specific test to determine whether a game is a game of chance or of skill and hence different criteria can be used to determine the same.⁵⁴ Fantasy sports are skill-based activities, according to studies conducted by several prominent academic institutions, including the Indian Institute of Management.⁵⁵

⁵¹ *State of Andhra Pradesh v. K. Satyanarayana & Ors.*, AIR 1968 SC 825.

⁵² *K.R. Lakshmanan (Dr) v. State of T.N.*, (1996) 2 SCC 226.

⁵³ *State of Bombay v. R.M.D. Chamarbaugwala*, AIR 1957 SC 699.

⁵⁴ *Supra* 4.

⁵⁵ Tech Desk, *Fantasy sports are skill dominant, finds IIMB-Cartesian study*, THE INDIAN EXPRESS, <https://indianexpress.com/article/technology/tech-news-technology/fantasy-sport-dream-11-iimb-cartesian-study-6165065/> (Dec. 13, 2019, 12:14 PM).

Researchers from the Massachusetts Institute of Technology (MIT) and Columbia University compared data from fantasy cricket and basketball platforms to stock market data. They concluded that fantasy sports players are more skilled than mutual fund managers who run stock portfolios.⁵⁶

Before 2015 fantasy sports were not considered to be a game of skill explicitly by any law or by any ruling of the court in India but in 2015, to promulgate a law which expressly placed such type of sports under the category of game of skill. The Nagaland Prohibition of Gambling and Promotion and Regulation of Online Games of Skill Act, 2015 established a licensed system for skill games and section 2(3) of the act specifically identified fantasy sports as a game of skill. However, after this Act, various Indian Courts in their judgments have ruled that fantasy sports are a game of skill and not a game of chance.

The Punjab & Haryana High Court, in *Varun Gumber v. U.T. Chandigarh*⁵⁷, held *Dream 11*'s gameplay skill-based, and stated that the gameplay of fantasy sports requires considerable skills, judgement, and discretion. The individual must calculate the potential worth of each athlete, taking into consideration their strengths and weaknesses when selecting the players. The factor of skill has the most significant influence on the result of the matches as the outcome is ultimately determined by how well the evaluation of the players is done by the participant.

In *Gurdeep Singh Sachar v. Union of India*⁵⁸ The High Court of Bombay observed that fantasy sports are different from betting, as winnability in fantasy sports had little to do with a team's performance in the real world. In the case of *Dream 11*, the participants make their own virtual team by selecting individual players according to their analysis. Hence, instead of the overall performance of the actual team, the performance of the individual players becomes essential. If that player does better in the live match, the participant will score points accordingly. The Court relied upon the judgement of *Varun Gumber v. U.T., Chandigarh*. It ruled that the activities and offerings of *Dream 11* (fantasy website) were legitimate and that they were not illegal gambling or betting operations disguised as online fantasy sports gaming.

⁵⁶ Vishal Misra et. al, *Is It Luck or Skill: Establishing Role of Skill in Mutual Fund Management and Fantasy Sports*, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, https://devavrat.mit.edu/wp-content/uploads/2020/08/report_skill.pdf (last visited May 9, 2021).

⁵⁷ *Varun Gumber v UT Chandigarh*, 2017 SCC OnLine P&H 5372 : 2017 Cri LJ 3827.

⁵⁸ *Gurdeep Singh Sachar v. Union of India*, 2019 SCC Online Bom 13059 : (2019) 3 AIR Bom R (Cri) 467.

The decisions of the Gurdeep Singh Sachar case and Varun Gumber case were challenged in the Supreme Court, which was dismissed immediately.

VIII. MEASURES FOR BETTER REGULATION OF FANTASY SPORTS

As emphasised by NITI Aayog the sector has a great potential to bring foreign investment and create jobs and hence fantasy sports need to be regulated in a better manner in order to get the best out of it. Presently there are many lacunas which can hamper the growth of the sector and removing these lacunas will result in the development of the sector and in turn will influence the nation's development. The following measures can be taken to ensure a better regulation of Fantasy sports: -

- Different laws for different states result in ambiguity which affects the functioning of such platforms so there should be a uniform law throughout the country regarding fantasy sports and the subject should be brought from the state list to the central list.
- There is a need for a separate recognition of online fantasy sports and the sector of online fantasy sports should be considered as a separate subject under the seventh schedule and should be separated from gambling which will result in better legislation and development of the industry.
- A separate regulatory body should be made at the central level to regulate fantasy sports and no regulation should be made at state level as it will create uniformity and which in turn will bring in foreign investment.

IX. CONCLUSION

Fantasy games are like a boon to the people who never get tired of talking about the technicalities and nuances of sports. Users of online fantasy game platforms have to weigh several variables, including the statistical success of the players, past records, weather conditions, among others, to be ahead of their competitors. Therefore, terming it as a guess work is not fair as it is a lot more than mere prediction.

For the most part, the fantasy sports industry is self-regulated by industry bodies like the All India Gaming Federation, ensuring that online gaming is conducted ethically. Nevertheless, gambling applications are at the whim of payment platforms and state governments, which can restrict an app based on “legislative ambiguity.” The Andhra government banned online gambling games by passing the amendment bill in 2020. According to Andhra Pradesh Home Minister M Sucharita, online gambling could encourage criminal behaviour in society and maximise the rate of organised crimes such as fraud and money laundering.⁵⁹

The Courts of law in the country have time and again judged that fantasy sports and games that include the performance of skills are out of the ambit of gambling. Thus, the Parliament has the option of passing legislation that can define, structure, and regulate the rules and regulations regarding fantasy sports and bring uniform law applicable throughout the country. The states will not have any right to question the legislation, as states’ right to make laws is limited to the matter of gambling and betting.

⁵⁹ PTI, *Andhra Pradesh Passes Gaming Amendment Bill to Ban Online Games*, NDTV, <https://www.ndtv.com/india-news/andhra-pradesh-passes-gaming-amendment-bill-to-ban-online-gaming-2332856> (last updated Dec. 2, 2020).

JURISPRUDENTIAL ANALYSIS OF LEGAL AND ETHICAL CONUNDRUM SURROUNDING ARTIFICIAL INTELLIGENCE

~ Mridull Thaplu & Monalisa Nanda¹

ABSTRACT

The issue of ethics revolving around Artificial Intelligence tends to be divisive and the contenders usually come from two fundamental basis of arguments, The first of them being the optimistic scientists who believe that their creation shall usher humanity into a new era of progression and the other one houses the pragmatist people of law and academicians who hold a rather conservative outlook of the same. The pre-emptive notion in the minds of the pragmatists is that AI shall always be inherently unsympathetic and calculative, thanks to the lack of a moral compass, and shall, in any given situation choose the more expedient option, without considering its ethicalities.

The legislative void surrounding AI has reinvigorated the jurisprudential debate of law reflecting human morality within itself. Most lawmakers agree on the setting up of a moral guideline to oversee the functioning of AI, but what needs to be addressed first, is the lack of legislations pertaining to the same. At present, India has no substantial legal base to rely upon, when it comes to AI. While certain developed nations do have legislations at nascent stages that act as supportive legal frameworks, the most substantial regulation upon AI is still maintained by the Three Laws of Robotics, that at best, are incorporeal. Thus, a holistically drafted umbrella framework needs to be enacted, that exists as a universal law governing AI, making the handling of AI, safer and undemanding.

Keywords: Artificial Intelligence, Jurisprudence, Ethics, Universal Legal System

¹ The co-authors are in their 4th year studying at Rajiv Gandhi National Law University

I. INTRODUCTION TO THE NUANCES OF ARTIFICIAL INTELLIGENCE

If the entire evolutionary process of planet Earth, starting from its very conceiving were to be condensed in a period of twenty-four hours, then human beings would not appear until the very last second of the said twenty-four hours. This not only puts into perspective the minuscule nature and the banality of human existence but also speaks volumes about how our actions have changed the face the Earth. Thus, the majority of the human world and its intricacies that exist around us came into being in the last thousand years. Out of these, only the past few hundred years have been immortalized thanks to the scientific and technological breakthroughs that were propounded during this time. The most significant human invention to have graced us is probably the creation of computers. Recently, the development of Artificial Intelligence has seemed to transmute the scenario completely.

Artificial Intelligence (hereafter, AI), is an extended branch of Computer Science that mainly revolves around producing machines that are capable of performing actions and achieving goals that were previously thought to only be possible by human ventures. As such, seemingly 'smart' technology paradigmatically changes the world as we know it. We are inevitably standing on the brim of a technological revolution, one that shall change the nature of human continuance forever. Without doubt, every ingenious innovation has its shortcomings that more or less depend upon how it is put to use. Similar is the case with AI, given that it is a technology that is self-driven and autonomous, the downfall of which is that it taps into the user's data to study his behavioral patterns to 'impersonate' him better. Being perfectly candid, the repercussions of AI are mostly ethical. They tend to go against basic human principles of goodwill which raise the question of whether we rushed into inventing something that we do not have the skill-set to regulate yet.

Stephen Hawking reflected that "*Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks.*"² Such apprehensions are not unfounded given the fact that the cosmic levels of intellectual prowess possessed by AI imply that if any part of our interaction were to go 'wrong', it would be irrevocably so and there shall be no recovering from such blunders. Thus, jumping head-on into such uncharted territory in order to relish the glory of human inventions is a folly, especially when it comes to these hyper-intelligent technologies.

² Rory Cellan, 'Stephen Hawking warns artificial intelligence could end mankind' *BBC News* (2 Dec 2014) <<https://www.bbc.com/news/technology-30290540>> accessed 25 August 2022.

The Evolutionary Growth of Artificial Intelligence

The idea of the existence of intellectual brilliance in non-human orientations was a mere fragment of human imagination that found its being in story tales, legends, and dystopian literature throughout the 19th and early 20th century. Such an idea was considered to be both awe-inspiring as well as scary and the aftermath of such hyper-intelligence was usually denoted as a threat to human existence.

British code-breaker Alan Turing who is regarded as a torchbearer in the field of technology in the 20th century did extensive research and published a landmark paper that talked about the possibility of creating machines that possess the ability to think and simulate human mind. His hypothesis was based on the fact that if human beings draw inspiration from pre-existing literature and studies as well as their environment and past experiences to solve complex problems, then a machine too, should be able to do the same, following similar *modus operandi*. For the very same purpose, he devised a test that helped in determining whether or not a machine is capable of thinking like a human being. This test went on to become one of the most extensively used control experiments in the field of AI.³ According to him, defining ‘thinking’ was an abstract thing to do, and thus, his experiment was designed in such a manner that it helped prove his hypothesis as a workable model. Notwithstanding the concrete proofs of his working hypothesis, he was ridiculed for having imagined something so whimsical. Later on, his experiments ushered humanity into a new area and the term 'AI' started its journey in the mid-1950s.⁴ There began the journey towards what was believed to be the most behemoth task in the history of mankind; creating something that was beyond imagination.⁵ This was followed by the Golden Era of Artificial Intelligence during the 90s wherein computers started making appearances in common households as hyperbolically smart gadgets.⁶ The gradual use of the Artificial Intelligence in almost all the fields requires transparency as well as accountability. In order for a system of checks and balances to be established and for such technology to be retained under human control, it is quintessential on our part to establish formal policy regulations to manage the same. In such circumstances, even the nature of the legislations so promulgated, need to be such that they

³ Alan M Turing, *Computing Machinery and Intelligence*, (Mind, LIX 1950) 433-460.

⁴ McCorduck & Pamela, *Machines Who Think* (2nd edn, Taylor & Francis 2004).

⁵ *Id.*

⁶ Turing (n. 2).

are holistic enough to act as a safety-net against any offshoots of AI while being flexible enough to not stand in the way of human dexterity.

II. JURISPRUDENTIAL ANALYSIS OF ARTIFICIAL INTELLIGENCE AND ITS LEGAL RAMIFICATIONS

In the dystopian classic, *Nineteen Eighty-Four*, George Orwell paints a rather bleak picture of how technology without mind, sentences human beings to their dooms while running on the commands of a despotic dictator. "Big Brother is always watching..."⁷, the novel reads, over and over again, but truth be told, had it not been for technology, such magnanimous control would have never been available to 'Big Brother' at the first place.

As Jacob Weisberg, a very famous Political journalist writes, "*Algorithms are developing their capabilities to regulate humans faster than humans are figuring out how to regulate algorithms.*"⁸ In such a scenario of impending doom, humans must hold back for a moment and reconsider their idea of AI which might end up obliterating the very notion of human ethics once it breaks the shackles of control of its human masters.

Though it is undoubtedly exigent to understand the ethical bearings of AI and the legalities behind the same, it needs to be established beforehand that even in the field of law, thinkers are divided between two schools of thought when it comes to the role played by morality within the *Rule of Law*. There exists a fundamental jurisprudential contention between the positivists and the naturalists on whether the law should reflect the circumstantial morality that guides the society. To oversimplify, legal positivists claim that one can say what the law is without making moral judgments about what it should be.⁹ Whereas, the naturalists are men of the old ways and believe that, for a law to qualify as 'good' law, it needs to stand up to a certain threshold of morality.

Furthermore, when it comes to the question of ethicality in AI, these two schools of thought seem engaged in a never-ending debate upon whether there should be a set of laws, guided by human standards of morality, to police the developments in technology or whether the

⁷ George Orwell, *Nineteen Eighty-Four* (Secker & Warburg 1949) 8.

⁸ Jacob Weisberg, 'The Digital Poorhouse', *The New York Times Review of Books* (New York, June 7, 2018) 47.

⁹ Joshua P. Davis, 'Legality, Morality, Duality', (2014) 1 ULR 61,63.

scientists should be allowed to play God on the particular subject and have autonomy upon how they want their creations to function.

Any discussion on the question of the ethicality of AI would remain incomplete if we were not to touch upon the problem of automated vehicles. While most car manufacturers would unflinchingly claim that their 'smart' cars shall prioritize human lives over the actual vehicle, the truth remains that though the AI would hold the driver's life in precedence, it would most likely not carry a duty of care for other commuters down the road or the pedestrians. Thus, if an automated car was to be faced with a situation in which he can either ram down five pedestrians or swerve the car right down a sinkhole in the road, thus killing the driver, it would spend no time considering the two sides of the situation and choose the expedient way out, i.e., kill the five pedestrians to save the driver. Undeniably, in such desperate circumstances, human minds would stop to consider the ramifications of their action of killing five people, in both, moral and legal senses and more often than not, human beings would try to find a middle ground between two bleak options in order to minimize the impact of the accident. However, once a machine is developed on a certain set of principles, it will not budge from the same because it does not possess the ability to think for itself. Thus, it will not be wrong to reflect that, programming them involves not just technical knowledge, it would seem, but also moral philosophy¹⁰. The Court was faced with such conundrum in the case of *Nelson v. American Airlines*¹¹ wherein injuries were suffered by the petitioner while one of the planes was on autopilot mode. The Doctrine *res ipsa loquitur* which means that “the thing speaks for itself” was applied by Hon’ble Court in the case of *Nelson v. American Airline*¹² for finding of the negligence caused while the airplane was on Autopilot mode. The court ruled out that the same can be rebutted if the Airlines could prove that Autopilot mode was not the main cause for the same; or there was some unpreventable reason behind the same.

¹⁰ Joshua P. Davis, ‘Law without Minds: AI, Ethics and Jurisprudence’, (2018) 5 USFSL 2.

¹¹ *Nelson v. American Airlines, Inc.*, 70 Cal. Rptr. 33 (Cal. Ct. App. 1968).

¹² *Id.*

III. LIBERAL JURISPRUDENCE: ALTERING THE CONVICTIONS SURROUNDING LAW

No matter how rosy or ingenious the entire arena of AI and its related sciences might sound, the reality is that they present a diverse multitude of problems when it comes to their legal implications, thanks to the ethical dilemma discussed above. If we were to continue with the example of the automated car and assume that the AI fitted within such a car did choose to run over the pedestrians in order to save the driver, then, whom does law hold liable for the death of the innocent men? How does the law pin the liability upon something that does not exist in the real world, but can actively choose to kill the five pedestrians? Can the concept of vicarious liability be made applicable to such a scenario? In general terms, vicarious liability is a specific type of liability that a supervisory party (such as an employer) bears for the actionable conduct of a subordinate or associate (such as an employee) based on the relationship between the two parties. As the software for the AI was designed and developed by the manufacturer who had absolute control over the actual manifestations of the AI, then will the manufacturer be held liable for the decisions made by his creation after the product is sold?

Given that AI can be designed in a way that it can overcome and vanquish the greatest of human intelligence models and establish itself as the one with higher acumen, should the establishment and interpretation of laws applicable to it, be left for itself to decide on its own? The idea behind such an argument is that human beings make and abide by said laws because they have enough rationale to do so and such complex behaviour is what sets them apart from other species. Similarly, the intelligence of AI is also unparalleled, so how long will it be before AI starts formalizing laws for itself? Though the very proposition of such an idea might sound preposterous, it is also true that time and again, technological developments have proved human beings wrong. Pundits once doubted that a computer would ever beat the world champion of chess because, the human mind, they argued—with its intuition—was simply superior¹³. However, now the greatest grandmasters of chess, rely upon the predictive models based upon AI to hone their skills at the game. Even in the Medical industry, there are automatic surgical instruments and treatment devices which have the capability and potential to diagnose and treat a person. However, the questions of liability, medical ethics, and medical malpractice still exist which may or may not encourage the use of these automated products in medical field and it is very difficult for a person to win suits relating to injuries

¹³.David Cole, 'The Chinese Room Argument' (*The Stanford Encyclopaedia of Philosophy*) <https://plato.stanford.edu/archives/spr2020/entries/chinese-room/> accessed 25 October 2022.

case of *Banker v. Hoehn*¹⁴ Wherein a plastic surgeon, undertook to remove the birthmark from the body of the person using Machines.

Max Tegmark, in his book, *Life 3.0: Being Human in The Age of Artificial Intelligence*¹⁵ opines that the work of judges in the judicial system is merely interpretive. He goes on further to shed light upon what he called, ‘robo-judges’ which according to him are, "AI systems that tirelessly apply the same high legal standards to every judgment without succumbing to human errors such as bias, fatigue or lack of the latest knowledge"¹⁶.

Next comes the question of the drastic change in income and employment dynamics when developed AI technology takes over the entire market. Business experts foresee that the entire hierarchy of blue-collar jobs shall come crashing down once the dominance of AI is reinstated in the field while most white-collar jobs shall stay secure as they more or less need human supervision. This basically means that extensive application of AI would lead to dilution of the job market that would inevitably result in the entrenchment of millions of workers and thus, the wealth disparity shall be greater than ever before. When it comes to the question of distribution of the wealth generated by the virtue of AI and allied technology, the working class is nowhere reflected in the equation. Consequently, individuals who have ownership in AI-driven companies would benefit disproportionately at the expense of the workforce which was eliminated as a result of AI.¹⁷

IV. SECURITY CONCERNS SURROUNDING AI: UNDOING HUMAN HISTORY

It is a common understanding that scientists develop AI in a manner that it closely reflects human interaction and behaviour pattern around itself. However, it is evident that no matter how impeccably designed the system is, it falls short of displaying human consciousness. Through this loophole, manifests a gap between the existence of robots driven by AI and human beings. It will not be unfounded to assume that after a given period of time, this gap would be so wide that the question would not be up to what extent robots can copy human beings. Rather, it would be, whether human beings would be able to customize their

¹⁴ *Banker v. Hoehn*, 278 A.D.2d 720.

¹⁵ Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence* (Vintage Books, 2017) 105.

¹⁶ *Id.*

¹⁷ Mirjana Stankovic et. Al., *Exploring Legal, Ethical and Policy Implications of Artificial Intelligence* (2017).

behaviour patterns to suit the interests of their robot counterparts. Through the medium of AI, the machines are now being given the status of human. In the past, too many companies, agencies and institutions have used ‘bots’ disguised as humans to influence/change the results and do the acts as specified. In the case of *Go2Net, Inc. v. C I Host, Inc*¹⁸, the court held that “*the parties’ contract permitted visits by search engines and other “artificial intelligence” agents, as well as human viewers, in the advertiser’s count of “impressions”*”.

While humans are limited in the attention and kindness that they can expend on another person, artificial bots can channel virtually unlimited resources into building relationships.¹⁹ We already see such real-life manifestation of human beings losing their behavioural control in Virtual-Reality (VR) scenarios that are embedded in games. The game tries to build circumstances that are addictive enough for the gamer to not let go of it and thus, gain control over human reactionary patterns.

The more powerful a technology becomes, the more potently it can be used for reprehensible reasons as well as good. This applies not only to robots produced to replace human soldiers, or autonomous weapons, but to AI systems that can cause damage if used maliciously.²⁰ If one were to go back in time and have a long and hard look at the wars that different human groups fought against each other in a mad-dash to establish their supremacy, one would notice that during a war, the quality of soldiers in an army is one of the deciding factors in the outcome of the war. When one side loses a major chunk of its soldiers, the mental prowess of the surviving soldiers suffers a blow and they usually end up losing the war. Thus, it would make absolute sense if AI is developed in a way that it compensates for the aforementioned human weaknesses and goes on to fight wars for its human masters. There was a famous case in relation to usage of Robots and Artificial Intelligence in the wars in early 90s in U.S known by the name *United States v. Athlone Indus*²¹, wherein it was stated that “*robots cannot be sued*”²² and instead the manufacturer has to be held liable for all the penalties and damage that has been caused due to the defect of the machine. In the near future the situations will change as AI will continue to grow and become more sophisticated than it is in the present time. The Courts will continue their struggle till the time a proper legislation/regulation is introduced answering the question of Liability and Standards, cases

¹⁸ *Go2Net, Inc. v. C I Host, Inc.*, 115 Wash. App. 73 (2003).

¹⁹ *Id* 13.

²⁰ *Stankovic* (n 16) 12.

²¹ *United States v. Athlone Indus., Inc.*, 746 F.2d 977.

²² *Id*.

that have been decided decades back also mirror the current legal framework revolving around the subject of risk caused through artificial and automatic intelligence.

V. LEGAL DEVELOPMENTS IN THE FIELD OF ARTIFICIAL INTELLIGENCE: THE WAY FORWARD

Laws governing human actions have existed for centuries, throughout different civilizations. However, the idea of the promulgation of laws to govern individual creations of human beings is rather novel and unheard of. Considering that AI is an emerging field and there are many risks involved in the same, the expanding horizons of the discipline is in itself putting great pressure upon governments. Bodies of authority all over the globe feel pressured to enact legislation for its regulation. Now, the real question is whether it is intelligent and viable in the long run to amend and modify the present laws in a way that suits robots driven by AI.

Even some bigwigs of the industry have felt the need for AI Regulation. Elon Musk in an interview said that the risks which are present in the field of AI are considerably high and normally set of rules are formed only when something bad happens because the government has to suppress the public outcry and thereafter it takes years for the formation of a regulatory body, same will be the case with AI.²³

Under the Fifth Report of the House of Commons Science and Technology Committee on Robotics and artificial intelligence, it was stated that there needs to be accountability for governing AI and managing the risks posed by it, *"While it is too early to narrow down sector-wide regulations for this nascent field, it is fundamental that cautious investigation of the moral, lawful and cultural elements of artificially intelligent systems starts now."*²⁴

In the year 2018, talks were held between France and Canada to establish a Global Governing body on the lines of the International Panel on Climate Changes. It was backed by the G7 countries, to study, analyze and put forward their opinions regarding effects of AI on the world, and the need and process to regulate the same. The nomenclature for the same was

²³ Samuel Gibbs , 'Elon Musk: regulate AI to combat 'existential threat' before it's too late' (*The Guardian*) <https://www.theguardian.com/technology/2017/jul/17/elon-musk-regulation-ai-combat-existential-threat-tesla-spacex-ceo> .

²⁴ House of Commons Science and Technology Committee report on Robotics and artificial intelligence [2017] ch 4, pr 71 5 HC 145.

changed in the year 2019 and was named 'The Panel for Global Partnership on AI'²⁵ whose main objective was to bridge the gap between the theoretical and the practical applications of AI which will act as a guiding force towards the holistic development of the field. These were adopted in June 2019.

In May 2019, the 'OECD Principles on Artificial Intelligence' were approved by the member countries and these were the first recommendations to be signed by individual governments. These principles were put forward so that the promotion of AI could be done in a broader and comprehensive manner. These recommendations were accepted by the member countries of OECD with the exception of Costa Rica, Peru, Ukraine and a few others. The OECD Recommendations on AI were based mainly on five value-based principles that are important for the proper regulation and differentiation between AI and human ethics²⁶. These recommendations focused on the development of a transparent law benefiting the stakeholders of society so that everything becomes crystal clear.²⁷

The World Economic Forum also issued its guidelines regarding the use of AI in government affairs which focused on safety and security issues. The Main draft legislation paper was prepared by the European Union²⁸ in early 2020 which was meant to promote and regulate the usage of AI throughout the world and had support from the UNICRI Centre for AI and Robotics.

Given the novel nature of the arena, combined with its intrinsic technicality, it poses a great problem in front of the legislators from both developed and developing countries. Many countries, as well as international bodies, have started drafting legislation, forming committees and strategic plans on AI which are in turn meant for the regulation, promotion, research and development of the field with respect to law.²⁹

In India, many attempts have been made by the government for development and promotion of AI. This has been one of the primarily prioritized fields of the overall development agenda because the government knows that this technology has the potential to make the lives of the

²⁵ 'Global Partnership on Artificial Intelligence' (*AmbaFrance, French Embassy in New Delhi*, 2020) <https://in.ambafrance.org/Global-Partnership-on-Artificial-Intelligence>.

²⁶ 'What are the OECD Principles on AI?' (*OECD* 2019) <https://www.oecd.org/going-digital/ai/principles/>.

²⁷ *Id.*

²⁸ European Commission White Paper on Artificial Intelligence-A European approach to excellence and trust [2020] COM (2020) 65 final.

²⁹ Jamie Berryhill et al., 'Hello, World: Artificial intelligence and its use in the public sector' (*OECD*, 2019) 72-74.

citizens easy and promote the dignity of labor and equality amongst the inhabitants of the subcontinent. There was sufficient allocation of funds by the government in the 2018 budget³⁰ meant for R&D in the field of Artificial Intelligence. The Union Government started a new initiative that went by the name 'Digital India', the main aim of which was to develop the nation on technological grounds and promote the indigenous manufacturing of logistical items. It is noteworthy to mention that research in the field of AI has been taken under this umbrella initiative.

An AI Task Force was set up in the country under the jurisdiction of Union Ministry of Commerce and Industry which was focused to *"implant AI in all the spheres of human thinking process of the citizens in the country- so that there is the fundamental ability to help the objective of India getting one of the pioneers of AI-rich economies"*³¹. The First report by AITF was released in March 2018 which identified some of the main sectors in the country which were lagging behind when it came to the utilization of AI. It also recommended the creation of a Nodal Agency to coordinate the activities related to AI in the country which would be known by the name 'National Artificial Intelligence Mission'. Loopholes were present in this report too because there was no thrust put on data privacy and issue of safety and ethics while using AI and it fails considerably while analyzing the tendency of the decisions which are made by machines having the probability of discrimination or biases.

In February 2018, the Union Ministry of Electronics and Information Technology established four distinct committees that were focused on the setup of AI in the country. The main aim of these committees was to create a proper roadmap for the development of AI in the country, headed by luminaries of the field that included directors of IITs. These committees were to be focused on Citizen-Centric Services; Data platforms; skilling, reskilling and R&D; Legal regulation and cybersecurity.³²

³⁰ Arun Jaitley's address to the Indian Parliament while presenting Indian budget for the Fiscal Year 2018. See, Indianbudget.gov at <https://www.indiabudget.gov.in/budget2018-2019/ub2018-19/bs/bs.pdf>.

³¹ 'Artificial Intelligence Task Force' (Ministry of Commerce and Industry, Government of India) <https://www.aitf.org.in>

³² Devika, 'Government releases — Artificial Intelligence Committees Reports' (SCC Online 2019) <https://www.sconline.com/blog/post/2019/12/05/government-releases-artificial-intelligence-committees-reports/> 10 October 2022.

The Legal Regulatory committee in its report that was released in December 2019 said that "A powerful legal system will be expected to manage those issues too complex or fast-changing to be addressed adequately by enacting a legislation"³³. The report recommended that the "stakeholders need to deliberate whether to perceive AI framework as a legal individual or not. On the off chance that legal status is given, it ought to be joined by an insurance scheme or compensation plans which will compensate if any damage takes place."³⁴

The Union Ministry backed think tank, NITI Aayog, had been tasked with drafting and producing national legislation which would be focused on regulating AI in the country. In order to achieve such ends, it signed an MoU with Google, ABB India, and a few other companies to integrate AI in the different fields of the economy and using the potential to the fullest.³⁵

Hence, we can reflect that the quest for the development of AI in the country has been in itself, a very tough and time-consuming one because the government has not yet created a regulatory body; a department which will provide legal insight into the matter, while committees have been formed only to coordinate and check whether the different sectors of Indian economy are equipped with the infrastructure to use AI in it. To be perfectly candid, however, the purpose of such committees is not fulfilled because the first step towards solidifying their operation, i.e., legislative regulations, does not exist yet.

1. Safeguarding Intellectual Property Rights

At the end of the day, AI too, like any other technological masterpiece, is a brainchild of its respective inventors and it is sheer injustice if their intellectual property rights are not protected just because AI is a novelty. Thus, to look into that matter, laws exist in our country and serve justice when it pertains to such issues. Though the laws exist in papers, their modalities do not really encompass the intricacies of the field.

³³ Report of Committee on Cyber Security, Safety, Legal and Ethical Issues [2018] Ministry of Electronics and Information Technology, Government of India.

³⁴ *Id.*

³⁵ Bureau, 'NITI Aayog, Google in partnership to grow AI ecosystem in India' (*The Hindu Business Line* 2018), <https://www.thehindubusinessline.com/news/niti-aayog-google-in-partnership-to-grow-ai-ecosystem-in-india/article23805535.ece>.

a. The Patents Act of 1970

Under Section 3(k) of the Patents Act, 1970 the computer programs or mathematical methods are not patentable *per se*³⁶ which means that they are categorized as non-patentable subject matters. A solo application for AI-Based Patent would not be entertained in the Patent registration office because such an application for a patent based on AI would not be a single invention rather it would be composed of one or more inventions. For patenting AI, the application needs to meet the parameters as set in the guidelines for Computer-related Inventions.

b. The Copyright Act of 1957

Under Section 13[o] of the Copyright Act, "literary work" includes computer programs, tables, and compilations including the computer³⁷ which means that the source code of the AI-based program made by the developer is protected and the Intellectual Property Rights of the same are vested upon the developer or the company where the developer of the program is employed. It further means that nobody can copy or use the source code of the program without the permission of the developer and he has the right to sue, defend and enforce his intellectual property rights if the same has been violated.

However, while laws do exist in the country regarding the Intellectual Property Rights of AI, we do not have a designated regulatory body nor a framework that talks about the regulation and working of AI. A proper legal definition for AI needs to be formed in accordance with Indian Criminal/Civil Law Jurisprudence which would provide the legal version of AI and answer the question of liability i.e., whether strict or absolute liability is to be enforced in the matters concerning AI.

2. Learning from the Experiences of Developed Nations

Given our nation's short-sighted dealing with technologies of tomorrow, it only makes sense for us to draw inspiration from the existing legal and regulatory framework of developed countries where they have been acquainted with such technologies for quite a while now.

³⁶ The Patents Act, 1970, No. 39, Acts of Parliament, 1970 (India), § 3(k).

³⁷ The Indian Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India), § 13(o).

The United Kingdom takes one of the most holistic approaches towards regulating AI on a global level. As the role of AI in the British Society has gradually increased, the government has looked deeper into the development and research work in the field of AI. The British undertook a two-fold method of approaching the new developments in AI; firstly, the impetus shall be upon creating awareness and resolving apprehension regarding the ramifications of AI; the next step shall be to recognize the importance of regulating the sector and developing comprehensive laws to guard against any fallouts. United Kingdom has its National AI Strategy which was signed in 2019 and is also known by the name AI Sector Deal³⁸ which contained many of the ideas that were given by Professor Dame Hall in its independent review³⁹.

The government formed a Committee on Standards in Public Life which was tasked with providing a complete report on the risks, regulations, laws required to govern in AI efficiently. The report of the aforementioned committee was published in February 2020, namely, *Artificial Intelligence and Public Standards Report* which said that instead of establishing a new regulatory authority or a new law, the existing laws should be molded so that they can look over the field of AI because the belief was that the English Legal system is enough to address the risks and the issues that come in development and working of the field. For the very same purpose, a Centre for Data Ethics and Innovation⁴⁰ was established and tasked with providing recommendations regarding the amendments required in the existing laws in the country.

Most of the European nations seem to have embraced AI and all its modalities whole-heartedly and have well-nuanced measures when it comes to the governance of AI. This is reflected through the European Union framework dictating the same. The European Union in its novel Plan of Actions to administer AI came up with the 'The European Strategy on Artificial Intelligence', an Expert Level Independent Group⁴¹ which was formed in 2018. It was tasked with providing guidelines regarding the regulation on AI including, but not

³⁸ 'AI Sector Deal' (*Policy Paper, The Government of the United Kingdom, 2019*) <https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal#key-commitments>.

³⁹ 'Growing the Artificial Intelligence Industry in United Kingdom' (*Executive Summary, The Government of the United Kingdom, 2017*) <https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk/executive-summary>.

⁴⁰ 'Driving Forward Trustworthy Data Sharing, Department for Digital Culture' (*Media and Sport, The Government of the United Kingdom, 2020*) <https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation>.

⁴¹ 'Report of High-Level Expert Group on Artificial Intelligence' (*European Commission, 2018*) <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>.

limited to policy development, addressing ethical and social issues, etc. Under the aegis of these guidelines, a 'White Paper on Artificial Intelligence' was published by EU in February 2020 that addressed the issues pertaining to Fundamental Rights, User Privacy, Data Breach and the Legal Liability. This was based upon two main ideas; "*ecosystem of excellence*" (to achieve excellence in all the fields) & "*ecosystem of trust*" (to comply with pre-existing rules of EU). The Commission concluded the report by reflecting that if any regulation is enacted, it should not be against the basic fundamental principles of the European Union.⁴²

The pre-existing laws in the EU shall apply to the field of AI, and the same shall be amended when needed because there are no specific legislations present to regulate AI at the very moment. The process of public consultation upon the white paper ended on 19th May 2020 and the Commission had collaborated with numerous luminaries in order to cover the legal aspect of AI in relations with comprehensively; *liability, IPR, ethics, Military use, etc.* and these reports will act as a medium to file a motion in the assembly to draw the attention to the matter which will prompt the Commission to start working towards enacting a legislation.

3. The Three Laws of Robotics: Paving Way for Universal Laws

In his stellar work, 'The Bicentennial Man', Isaac Asimov laid down the famous Machine Ethics, also known as the 'Three Laws of Robotics'. The rules pertain to the maintenance of a certain degree of required ethicality on the part of machines in order for them to be deemed intelligent in real sense. The work was originally published in a collection of stories that were listed to commemorate the fulfilment of two centuries worth of existence of the United States, and Asimov's work made an everlasting impression through the same by his proposition that machines shall completely change the thought process and behavioural patterns of human beings in the upcoming years. Asimov's Three Laws read as:

*"Firstly, a robot may not injure a human being, or, through inaction, allow a human being to come to harm. Secondly, a robot must obey the orders given it by human beings except where such orders would conflict with the First Law. Lastly, a robot must protect its own existence as long as such protection does not conflict with the First or Second Law."*⁴³

⁴² (n 26) 16.

⁴³ Isaac Asimov, 'The Bicentennial Man', *Philosophy and Science Fiction* (M Philips ed., Prometheus Books, 1984).

The aforementioned laws, though platonic in a real sense, suggested at a higher form of relationship between human beings and robots. He, thus, explained why humans feel the need to treat intelligent robots as slaves, an explanation that shows a weakness in human beings that makes it difficult for them to be ethical paragons.⁴⁴ Therefore, based on a similar line of reasoning, it would not be incorrect to propose that while amending municipal laws to regulate the inappropriate use of AI is legitimate, imposing such rules on the AI itself may be crossing a morally precarious line. In such a case, it would make sense to have a basic set of laws like those proposed by Asimov at a universal level while giving enough space for AI to function as independent intellectual beings of their own.

Such a universal set of laws shall be the founding cornerstone of jurisprudence upon the existence of AI. It shall honour them as individual beings, independent of their human creators, and shall address them as inherently rational individuals with high intellectual capability. Primarily, such universal laws would not only exist to check the behaviour of robots but would also make sure that heinous human instincts like that of enslaving another being, are not reinvigorated as we step into a new technologically advanced era.

As is the case with any new technology, it will not come as a surprise if a few developed countries get into a mad dash of weaponizing the same. Thus, in order for another century's worth of warfare to be kept at bay, it would be a rather ingenious idea for the entirety of laws governing AI to be international, thus, effectively checking selfish usage of such intelligent technology by short-sighted nations or hedonistic governments.

VI. CONCLUSION

If one were to take dystopian literature as the parameter for determining the nature of the relationship between human beings and robots, then the scenario would be quite dismal and pessimistic, because the conviction shall always be that human beings need to be wary of such intelligent technological beings. However, the reality is way less scary than the popular narrative and the only pressing question in front of us is whether human beings should decide a level of moral standards and laws for robots or if they should be allowed to govern themselves on their own accord, considering their intellect. The prospect is not quite as

⁴⁴ Susan Leigh Anderson, *Asimov's "Three Laws of Robotics" and Machine Metaethics*, (UCP, 2005).

apocalyptic of computer programs interpreting our laws for us, and perhaps taking over as our judges, awarding damages, and even imposing criminal sanctions.⁴⁵

To sum things up and put them in proper perspective, to date, as stunning as technological developments have been, they seem to run along the lines of description and prediction—of identifying patterns in service of prescribed goals—but not of identifying goals worth pursuing.⁴⁶ Thus, on similar lines of argument, one can say that even if AI does end up surpassing human beings in every field imaginable, their actions would have different ends than ours and rather undeniably so, our actions shall reflect generations worth of indoctrination and life lessons. In contrast, theirs shall reflect nothing but algorithmic programming.

Legal Dualism suggests a potential resolution to that debate.⁴⁷ Legal Dualism in this scenario more or less refers to a legal system based on both, normativism and positivism. If human beings were to retrace their steps, then they would see that nascent legal traditions drew their inspiration from the 'Law of Nature' and the entire judiciary was more or less based upon convictions associated with good and bad that defined the moral standards. While such systems were more or less replaced with the advent of Machiavellian modern political thought, the proliferation of AI might mean that we need our traditions up and alive. So, an actual system of organic balance can only be achieved if human beings take up the more 'humanistic' part of legal interpretation that involves morality and conscience. In contrast, AI can impose upon itself a legal code that shall oversee the more 'technical' and inorganic aspects of its functioning. The aim of integrating AI into the legal system should be to further the scope of jurisprudence while making sure that the AI itself functions within the ambit of such legal philosophy, thus creating a virtuous cycle of sorts.

⁴⁵ Davis (n 8).

⁴⁶ *Id* 40.

⁴⁷ Davis (n 8) 40.