THE LEGAL JOURNAL ON TECHNOLOGY

SILICON AND PRECEDENTS

JOURNAL | SPRING ISSUE

2025

VOLUME 1
ISSUE 2

THE LEGAL JOURNAL ON TECHNOLOGY

IN THIS ISSUE

- AI ON SOCIAL MEDIA
- QUANTUM TECHNOLOGY
- DEEP FAKES
- VIRTUAL RAPE
- AI LIABILITY
- NFTS
- DATA & CONSUMERISM

EDITORIAL BOARD

ADVISORY BOARD

FOREWORD

It is slightly more than one year since I was put in charge of The Legal Journal on Technology.. During such time, the Journal has gradually outgrown its initial conception as an Internet-based discussion world and started to establish itself as the site upon which legal issues of technological change can be addressed in a sustained and serious way. The desire to do this has been guided by a mere belief that the legal study should not stand behind, facing the technological landscape with unflinching clarity, rigor, and intellectual integrity. It is an Expression of the same devotion--to develop new tones, to deepen the critical acumen, to add to literature without at all spoiling its own ease the burden already borne by previous generations.

“Death to Videodrome! Long live the new flesh!” - Videodrome (1983)

That line is gloriously unhinged, but it captures something real about our moment: law is being forced to meet “new flesh” every day, in the form of fast-moving technologies that reshape power, privacy, markets, and speech before doctrine can catch its breath.

With this second issue, our aim was straightforward: publish work that does more than describe technology’s rise. Each piece has been curated to push analysis forward, to argue carefully, and to stay usable for students, researchers, practitioners, and anyone trying to think clearly inside legal uncertainty. This issue is also a step in strengthening the journal’s institutional footing. After this publication, we will be applying for an ISSN, so our work is more formally indexed, citable, and discoverable.

This is followed by opening the Issue, **Assessing the Impact of Artificial Intelligence on Social Media Dynamics: Prospects and Challenges**, which questions how temporary systems determine the speech, participation, and influence in the digital masses communication. The article discusses efficiencies promised by AI-powered platforms as well as regulatory anxieties that it generates especially in context of manipulation, accountability and democratic discourse.

Quantum Technological Era: Legal Shifts and Challenges shifts to a new frontier, in which the field of legal scholarship fortunes to have uncovered so little. Through the perspectives of cybersecurity, data protection, and regulatory preparedness, the article shows that the changes in quantum computing are deep-rooted doctrinally and institutionally and may be necessary in the near future.

The Journal asks a question that is very unsettling, yet at the same time, badly needed. Whether current criminal and child-protection systems are conceptually prepared to deal with the harm that occurs in immersive virtual spaces, and whether legal standards need to be reconfigured are questions that are explored under the article titled **Can the First Ever Registered Virtual Rape Change Legal Standards for Minors in the Metaverse?**.

FOREWORD

In **The NFT Paradox: Ownership Without Rights?**, the author examines the complexities of the digital ownership. A Maze of Overlapping Claims, that slices the discontinuity between technological claims of proprietorship and legal state of intellectual property, licensing, and control in tokenized space.

With an effective and timely analysis of competition law in data-driven markets, the Issue is **Balancing Data, cartels and consumerism Against Anticompetitive Practices**. The article challenges the need to understand how old antitrust values need to be modified in the face of platform economies, where data concentration, collusion, and consumer harm are coming into contact in new ways.

AI Liability: Solving the Attribution Problem in Autonomous Systems addresses the most intractable issue of technology law: the distribution of responsibility when two different actors, both human and machine, share the decision-making process. The author cautiously explores the issue of fault, causation, and accountability in the area where the conventional models of liability have started to toll.

The Issue concludes with a longstanding but much more pressing issue in **Reinforcing Legal Safeguards against Deepfakes: Examining the Regulatory Approach in India**. The article leaves the realms of abstract alarmism and takes a critical view of the current Indian legal mechanisms and finds the loopholes that require a legislative and policy response in the light of a fast-growing synthetic media

Collectively, the following seven articles can be seen as a reminder that this Journal is about being a serious, analytically-based forum, which does not view technology as a new phenomenon, but rather as a continuum that is continuing to change legal thinking. I do praise the authors with their thorough research, their audacity to explore tough questions and their readiness to be clear on the aspects where conceptual vagueness is rather common.

This is in hopes that this Issue will be useful not just to lawyers and policymakers, but to technologists, scholars, and readers interested in the future of fair, accountable and responsive legal systems. We welcome debate, discussion and additional research, as is part of our mission to sharpen knowledge and to make a positive contribution to the current rapidly changing relationship between law and technology.

Warmly,
Rudraditya Singh Panwar
Chief Editor
The Legal Journal on Technology

FOUNDERS NOTE

As we release Issue II, I'm genuinely proud of what TLJT has become. What started as an idea has grown into a serious publishing effort, and a lot of that credit goes to my little brother, Rudraditya, who has built this into something real with consistency, discipline, and sheer work ethic.

A special thank you to Anjuli and Rasleen for managing the moving parts behind the scenes and keeping the team and timelines on track.

This issue reflects our intent: clean, relevant, and rigorous writing on technology law that respects both scholarship and the reader.

And as the internet philosophers would say: "We're so back."

Aryaman
Founder, The Legal Journal on Technology (TLJT)

TABLE OF CONTENTS

Assessing the Impact of Artificial Intelligence on Social Media Dynamics: Prospects and Challenges

- **Dr Ankita Kumar Gupta[*] & Ms. Arsheya Chaudhry[**]**

Abstract

The branch of computer science known as artificial intelligence studies how well a machine can replicate human intelligence. It could assist in addressing some of the most difficult socioeconomic issues faced around the globe today and could do wonders. These days, social media also referred to as social networking consists of YouTube, Facebook, Instagram, Pinterest, Twitter etc. AI is essential to the operation of today's social networks. AI is being used in social media in ways that have never been seen before, and it is rapidly changing the platform. In the recent few years, social networking site usage among Indian internet users has increased dramatically, especially among younger generations. Additionally, the use of AI by social media has presented various difficulties for the Indian law enforcement agencies. Therefore, comprehending the application of artificial intelligence in social media and its consequences is crucial. With the right knowledge of artificial intelligence and social media, including its advantages and disadvantages, the Indian legal system can use the potential of these technologies to address contemporary issues. Given the misuse of social media, content monitoring has become essential. The paper presents SWOT analysis of the use of AI in social media trying to answer whether AI and social media are bone or bane.

Keywords: Artificial Intelligence, Social Media, Deepfake, Legal Reforms.

I. Introduction

Artificial intelligence (AI) is a technology that imitates human behaviour and gives gadgets intelligence. It is distinct from other recently developed technologies since it can alter human nature, Al is regarded as transformative technology. Nevertheless, there hasn't been a consensus definition of Al up until now, it is a ubiquitous technology that has impacted our daily existence.[1] The cognitive science of Artificial Intelligence studies intelligent machines that can carry out tasks that were previously solely done by humans. Its primary focus is on using computers to perform activities that depends on cognitive, perceptual, reasoning, and comprehending skills. Individual behaviours, tastes, opinions, and

[*] Assistant Professor (Senior Grade), Vivekananda School of Law and Legal Studies, Vivekananda Institute of Professional Studies-TC, New Delhi, Email: ankita.gupta@vips.edu

[**] Perusing LLM in IPR and Technology Laws, O. P. Jindal Global University, Sonipat, Haryana. Email: 24jgls-achaudhry@jgu.edu.in

[1] Chemmalar S, 'Artificial Intelligence and Legal Implications: An Overview' (2018) 14 National Law School Journal <https://repository.nls.ac.in/nlsj/vol14/iss1/14>.

interests can be leveraged by AI systems through training to personalise experiences. Machines can be trained to mimic human behaviour. They can provide them the capacity to hear, see, move, write, and speak. AI is far more adept than humans at picking up these habits. Numerous sectors are using AI technologies to automate and improve the efficiency of a range of jobs.[2]

II. Application Of AI in Social Media

A variety of web-based and mobile systems that enable users to produce and share digital content are collectively referred to as "social media." Digital material can be text, photographs, music, movies, and places, among other formats.[3] Social media has become a part of our everyday lives, with billions of people sharing massive amounts of data on sites like Facebook, Instagram, and Twitter on a regular basis. AI algorithms are used to analyze this data and behavior in order to give customers personalized information. Through the analysis of user-interacted articles, pages, and biographies, AI can identify patterns and recommend new content that people might find interesting. Content curation is a technique used to keep users engaged and entice them to stay on the platform longer.

Artificial intelligence has the potential to significantly alter how firms advertise on social media sites like Facebook, Instagram, Snapchat, Twitter, and LinkedIn. Campaigns, social media ads, and events may all be developed and targeted with it. It can automate regulation and powers the majority of content on social networks. At present, social media marketers may leverage this unadulterated technology to achieve incredible and long-lasting outcomes. The smartphone's voice assistants and real-time navigation are powered by AI. Online retailers, such as Netflix and Amazon, employ AI to recommend products and content. Email systems like Gmail even employ artificial intelligence to compose parts of your emails automatically.

Machine learning, a subfield of artificial intelligence that allows computers to reliably predict outcomes from massive volumes of data, which drives artificial intelligence's most impressive features. It is the most cutting-edge artificially intelligent tools available, whose forecast accuracy is getting better because AI can learn to get smarter on its own, often without human input, as it is incredibly powerful. Massive amounts of unprocessed data are used by AI technology nowadays to forecast increasingly relevant and precise outcomes, such as what product one should buy next, what advertising campaign to conduct, and what subjects to write about in a blog

---

[2] Matthew NO Sadiku and others, 'Artificial Intelligence in Social Media' (2021) 2 International Journal Of Scientific Advances <https://www.ijscia.com/?p=1906> accessed 10 February 2025.

[3] Muktesh Chander, 'Social Media: Analysis of New Challenges and Opportunities for Indian Law Enforcement Agencies' (2024) 2014 Indian Police Journal 123.

based on previous searches. Artificial intelligence can read and write through natural language processing and synthesis. It uses the sentiment analysis step to identify speech tonality. It recognises people, images, and videos using a variety of image recognition algorithms and computer vision techniques. AI is even able to forecast performance and suggest actions. And, by utilising these features, one can give the social media marketing superpowers and raise customer engagement.[4]

In order for social media platforms to function today, artificial intelligence is essential. Popular social networks such as Instagram, Facebook, LinkedIn, and others employ machine learning models to recommend users or accounts to follow, recommend jobs, identify photographs, monitor conversations, and do other similar functions. Artificial intelligence is used by several of the most well-known social networks that we utilise on a regular basis. Facebook employs more sophisticated forms of artificial intelligence and machine learning to display postings, among other things. They resemble those that a user has already interacted with. They can send pop-up advertisements, identify faces in tagged photographs, and so on. Facebook is the owner of the social networking site Instagram. To locate and remove phoney posts from user accounts, it employs AI. Snapchat tracks the traits of its users' faces in real time and adds effects that move with those features by using computer vision, a sort of artificial technology. LinkedIn leverages artificial intelligence for a variety of functions, including automated bidding, job recommendations, suggested connections, specialised content delivery in feeds, audience targeting assistance, and conversion tracking. The personalised content that Pinterest displays is a big part of why so many people adore it. Instead of typing in keywords, users can take photographs using Pinterest Lens and use them to search for relevant products. Because Pinterest provides hyper-personalized content, more than 80% of its active users make purchases through the platform.[5]

III. Hazards of Artificial Intelligence in Social Media

While AI has the potential to address some of the most difficult societal issues facing humanity, it is not a panacea. The possibility for privacy infractions in social media is one of the main hazards associated with AI. Social media sites have access to a great deal of personal data since AI algorithms use user data to personalise content and recommendations. Anything from location and search history to likes, shares, and comments might be included in this data. Although social media companies assert

[4] Trupti Bansode and others, 'A Review On Impact Of AI On Social Media' (2024) 12.
[5] Preeti Singh and others, 'Implications & Impact of Artificial Intelligence in Digital Media: With Special Focus on Social Media Marketing' (2023) 399 E3S Web of Conferences 07006.

that they safeguard user privacy, there have been multiple cases of data breaches and improper use of user information in the past few years.[6]

The dissemination of false information on social media for political and social purposes is another issue. For nefarious political or financial purposes, a person could disseminate photos or films that were not authentic. Because so many politicians use forums to spread their opinions among the public, this dread has come to pass. The presence of AI-generated images and videos, AI voice changers, and fake news into political and social spheres has made online media and news even more depressing. Thanks to these technologies, users may easily generate realistic images, films, and audio snippets, or replace a current image in an existing picture or video with a new one and this technology is called "Deepfake".

Deepfake is a type of artificial intelligence (AI) technology that uses machine learning techniques, particularly generative adversarial networks (GANs), to produce synthetic media, such as images, videos, and sounds. The goal of deepfake technology is to create incredibly lifelike synthetic media that, with some content alteration, resembles real people. Deepfake technology is proliferating and ending up in the hands of unscrupulous people. Misuse of this technology can take the shape of dishonest business dealings, fictitious depictions of well-known individuals, and, in the worst situation, extortion. Over the last ten years, deepfake technology has advanced at an alarming rate and may be broadly classified into three categories:

a. Face switching - Face swapping is the practice of substituting another person's face for one's own in images or videos.

b. Lip Syncing - In audio or video content, lip syncing refers to the process of making someone appear to say something they did not say.

c. The puppet technique - This method describes the fake, phoney movements of a person.

Today, public at large is negatively impacted by Deepfake technology. Indian authorities recently dealt with their first case of impersonation using deepfake technology, which occurred in July 2023. An old man was conned out of his savings account by his bank when he received a deepfake video call from an AI-generated account that looked like it was from a colleague and asked for a big payment. Verification revealed that the video was a deepfake and that the aforementioned coworker was not aware of the

[6] 'The Biggest Data Breach Fines, Penalties, and Settlements so Far | CSO Online' <https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html> accessed 10 February 2025.

video conference.[7] The issues with deepfake technology were once again brought to light when Bollywood actress Rashmika Mandanna's deepfake video began to circulate on social media.[8]

There are numerous ways that deepfake technology can be utilized to commit crimes. Although it can be used as a weapon to commit crimes against society as a whole, technology is not intrinsically dangerous. Crimes like identity theft and virtual forgeries can be perpetrated through the usage of deepfakes. These are grave offenses that have the potential to profoundly impact a person's life as well as society at large. By adopting another person's identity, fabricating personal narratives, or swaying public opinion, deepfakes can be used to disseminate misleading information and damage someone's credibility and reputation. Deepfake online defamation and hate speech can also be severe problems that hurt individuals and society at large. Deepfakes can seriously damage people's reputations, well-being, and online communities when they are used to disseminate hate speech or libellous content. Additionally, this technology can be used to create phoney images or videos of people saying or acting in ways that never happened, which could damage people's reputations or spread false information. Deepfakes may also be maliciously used for non-consensual pornography, political propaganda, or disinformation operations. Deepfakes can be harmful to society at large as well as the people whose images or likenesses are utilized without permission when they are used to spread false information or influence public opinion.

IV. Legal Reforms for Deepfake AI Technology

Currently, India lacks in providing a specific law on Deepfakes and AI related crimes. But there is a plethora of different legal provisions that can provide for civil or criminal relief. Such as the defamatory laws in India, both criminal and civil law, can hold someone accountable for defamatory acts. Cyber defamation is the broadcasting of false information about another individual via the internet or computers. Cyber defamation occurs when someone posts a defamatory comment about another person on the internet or sends emails conveying the same to other people with the goal of discrediting the target of the statement.[9] In civil law, defamation is

---

[7] 'Kerala Man Loses ₹40k to AI-Enabled Deep-Fake Fraud' (*Hindustan Times*, 18 July 2023) <https://www.hindustantimes.com/india-news/deepfake-scammers-trick-indian-man-into-transferring-money-police-investigating-multi-million-rupee-scam-101689622291654.html> accessed 10 February 2025.

[8] 'Rashmika Mandanna Deepfake Case: Delhi Police Writes to Meta to Give Info of Account That Shared Video' (*Hindustan Times*, 11 November 2023) <https://www.hindustantimes.com/entertainment/bollywood/rashmika-mandanna-deepfake-case-delhi-police-writes-to-meta-to-give-info-of-account-that-shared-video-101699689506970.html> accessed 10 February 2025.

[9] Aswathy Ph.D, 'A Critical Study on Cyber Defamation and Liability of ISPS' (2018) 119 International Journal of Pure and Applied Mathematics 1717.

punishable by the tort law, which states that if the defamatory act is proven to have occurred, the person who was defamed will be entitled to damages. On the other hand, Section 499 of the Indian Penal Code, 1860, defines Defamation. According to this section, Defamation is a punishable offence and can result *"from publishing any material that could be construed as harming someone's reputation"*. Section 500 of the Indian Penal Code, 1860, stipulates the punishment for the same offence, which consists of *"a fine, a maximum two-year prison sentence, or both"*. These regulations are still in their infancy and cannot handle the variety of deepfakes that are currently in existence.

Cyber defamation was covered by previous cyber law as well, which was codified in Section 66A of the IT Act.[10] The clause specifically addressed any derogatory content delivered via a computer source with the intention of obstructing, offending, hurting, inciting hatred, intimidating criminals, or sowing discord. But this clause was removed from the IT Act as the Supreme Court invalidated it in the Shreya Singhal case.[11]

Section 66E of the IT Act presently applies to deepfake offenses that involve the acquisition, distribution, or publication of a person's image in the media, violating that person's privacy. This type of violations warrants a fine of ₹2 lakh or a jail sentence of three years. Similarly, Section 66D of the IT Act punishes those who maliciously use computers or communication devices to impersonate or deceive others. A violation of this provision carries a maximum sentence of three years in prison or a fine of ₹1 lakh.

Additionally, violating Sections 67, 67A, and 67B of the IT Act may lead to legal prosecution for transmitting or broadcasting pornographic or sexually explicit deepfakes. The IT Rules also prohibit hosting "any content that impersonates another person" and require social media companies to take down "artificially morphed images" of people as soon as they are alerted. They risk losing the "safe harbour" protection, which exempts social media companies from legal responsibility for user-generated content on third-party platforms, if they fail to take down the aforementioned content.

Deepfake content occasionally includes modified audio and visual elements from movies or music videos that may be copyrighted. According to Section 14 of the Copyright Act of 1957, the owner of the cinematographed music video or film has the exclusive authority to provide a licence for the creation of another copy of the work, including any image or sound that is represented by a picture or photograph. The author's moral right was acknowledged in the Delhi High Court case of Amarnath Sehgal v. Union of India. In the event that his honour is violated or his moral rights over his creation are violated, the author is entitled to damages for any act of mutilation, distortion, or change. If the moral rights

[10] Information Technology Act, 2000.
[11] *Shreya Singhal* v. *Union of India* A.I.R. 2015 S.C. 1523.

of his licenced work are violated, the copyright owner may be entitled to civil remedies such as an injunction, damages, or other remedies granted by the law. In addition, anyone found to have intentionally assisted in the infringement of a copyrighted work or any other rights granted to the copyright owner under the provisions of the Act faces up to three years in prison and a fine of up to two lakh rupees. However, these remedies might not be effective for the victim of a deepfake content because, generally speaking, it is believed that the producers of films own the copyright, not the actors, who run the risk of becoming targets. This also holds true for pictures and photographs, where the owner of the copyright is the photographer, not the subject of the picture. Therefore, neither the target of the deepfake content nor the real victim may benefit from the remedies offered by this act.

In the Justice K. S. Puttaswamy v. Union of India[12] case, the nine-judge bench acknowledged that an individual's right to privacy is protected under Part III of the Indian Constitution. The case centred on the individual's right to sue the State and non-state actors for infringements on their informational privacy, which acknowledges the individual's control over their personal and digital privacy. Therefore, utilising a person's private or intimate information such as pictures or videos to create non-consensual deepfake content about them is a violation of their fundamental right to privacy.

A historic piece of legislation was enacted in the shape of the Digital Personal Data Protection Act, 2023 (DPDPA) which seeks to protect people's privacy in the digital age. It aims to establish a comprehensive framework for India's legislation pertaining to the protection of personal data. All organizations that handle the personal data of Indian persons are subject to the Act, which went into effect on September 1, 2023. The DPDPA attaches a Data Principle's obligations under Section 15 of the Act. Section 15(b) restricts the common problem of impersonation. This is important in light of AI-generative media, which is frequently used to deceive people by posing as someone else. Data Fiduciaries can track out the origin of a deepfake and hold the individual who uploaded it to the website accountable after receiving a complaint. This clause allows for action to be taken while providing the injured party with enough time to recover. However, this technique is only helpful when a person can be located using a unique identifier or a unique account on a data fiduciary platform. If this person impersonates someone else using a deepfake, they could be prosecuted for breaking Section 15. If it were difficult to identify the video's origin or link it to a specific individual, the clause would essentially be irrelevant.

[12] 2017 10 SCC 1.

V. Global Scenario

Deepfakes pose a serious risk to society at large, and as artificial intelligence has advanced, so too has its potential for evil. With the advancement of deepfake technology, it is now much easier to alter reality representations. Numerous social, economic, and psychological issues are brought on by deepfakes. India currently lacks a strong criminal legislation or civil liability framework that can directly address the problems associated with the production and dissemination of deepfake content. In a 2019 draft on intellectual property policy and artificial intelligence, the World Intellectual Property Organization (WIPO) addressed two specific concerns with deepfakes. This was accomplished in an indirect manner. The WIPO asserts that deepfakes have the potential to cause more significant issues, such as violations of human rights, privacy rights, and the protection of personal data, as opposed to copyright violations.[13]

a. Deepfake regulations in USA

The United States of America was in the forefront of the response to the advancement of artificial intelligence technologies. In 2018, the Malicious Deep Fake Prohibition Act was passed by the US Congress. This legislation is important since it is the first attempt to define the phrase “Deep-fake” legally. In 2019, the DEEP-FAKES Accountability Act was formally presented. The production and dissemination of deepfake films were outlawed in Texas in 2019, making it the first state in the union to do so. Following that, two laws were passed in California in 2019 that gave victims of deepfake, nonconsensual pornography the ability to sue for compensatory damages. The creation and distribution of non-consensual deepfake pornography are now crimes in Georgia and Virginia. Legislation connected to the pursuit of legal remedies against the unapproved spread of deepfake content was passed in New York in 2020.

b. Deepfake regulations in EU

The European Union (EU) is pushing for increased research efforts in the fields of deepfake identification and prevention, taking a proactive approach to the regulation of deepfakes. The European Union's Artificial Intelligence Act, 2024, has adopted a proactive approach in the fight against deepfakes. Furthermore, in order to combat deepfakes, the EU had previously suggested legislative provisions requiring the open labelling of artificially generated content, which have been appropriately acknowledged by the recently passed AIA. A thorough study titled "Tackling online disinformation: a European Approach" was issued by the

[13] ‘Artificial Intelligence and Intellectual Property Policy’ <https://www.wipo.int/about-ip/en/artificial_intelligence/conversation.html> accessed 10 February 2025.

European Commission in 2018. It featured a number of measures aimed at preventing information providers from unlawfully influencing public opinion.[14] In 2021, the Future of Science and Technology Panel conducted research and produced a report titled *"Tackling Deep-fakes in European policy."* The report detailed various aspects of the deep-fake lifecycle that policymakers could take into account to address and lessen the adverse effects of deep-fakes.

The General Data Protection Regulation (GDPR) of the EU has strict restrictions on deep-fakes. The definition of "personal data" in Article 4(19) of the law *is "any information that pertains to a specific or identifiable individual."* Given that a deepfake can be readily identified as a real person, it surely falls under the GDPR's purview if it does so. The EU has created the first comprehensive AI law in history, and it appears to be well-positioned to address the growing threat posed by deepfakes. This is in addition to the several regulations and initiatives now in place that attempt to incorporate deepfakes into the current legal framework. By taking these steps, the application of deepfake technology is limited with respect to artificial intelligence regulation, personal data protection, and misinformation governance. The most important AI regulatory framework for law enforcement in deepfakes is being developed by the European Commission, and its implementation is anticipated. Legislative steps have also been implemented by the EU to require social media companies to remove misinformation, including deepfakes, from their platforms.

VI. Conclusion & Recommendations

Technology is constantly evolving. There is a new development in the field of technology every day. AI is utilizing one such technology that has become popular. A wide range of technologies, such as computer vision, robots, expert systems, machine learning, natural language processing, and more, are referred to as "artificial intelligence." A lot of businesses are already aware that AI is the route to go in order to advance their operations. As AI advances and changes, social media networks will continue to be impacted by it. The possibilities are endless when it comes to AI in social media. Businesses have found social media and AI to be a particularly beneficial combination.

Deepfakes will continue to evolve and become more complex in the near future, which will raise concerns about how they might impact society. As AI algorithms advance, it becomes harder to distinguish between authentic and fraudulent content, which affects people, privacy, and trust. The

[14] ' Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236> accessed 10 February 2025.

likelihood of losing trust in digital content is rising as deepfakes become more realistic. When individuals begin to question whether any image or video is authentic, there may be a generalized sense of skepticism. This could have important ramifications in high-stakes domains like justice and law enforcement, where the integrity of the evidence is vital.

The spread of deepfake and shallow content highlights the need for sophisticated software and laws while also illustrating the evolution of deepfake technology. Examining synthetic media will require collaboration by lawmakers, IT developers, and the general public in order to achieve a balance between innovation and safeguarding against detrimental misuse. By doing this, we may all cooperate to safeguard the integrity of our digital environment and mitigate the negative consequences of deepfakes. When it comes to AI, the existing restrictions are insufficient. The legal system does not meet the needs of emerging technologies as it stands. Here are some suggestions to maintain the constant urge:

a. The state's existing laws against defamation, identity fraud, data theft, privacy, copyright, etc., should be reinforced in order to combat the crimes linked to deepfakes. Strict sanctions and punishments for creating deepfake content may act as a check on the pace of technology development and the dangers it presents to society. It is necessary to pass laws that are directly related to AI and Deepfake technology.

b. When users encounter deepfake content on their network, social media apps, and service providers can develop and put techniques into practice to alert them. The terms and conditions of the service providers' privacy policies must set a limit beyond which they are unable to misuse the data and privacy of their customers.

c. Fighting deepfake content also requires education and awareness. The general public ought to be made aware of deepfake content and the potential risks associated with this AI-generated technology. Creating awareness among people not to share or promote any fake content online is another important aspect. The general public should be made aware of how to spot deepfake content that can be found on internet media platforms.

Well-known platforms like Facebook, Twitter, TikTok, Instagram, Snapchat, and others that let users upload and share content also have moral and societal obligations to forbid or restrict the publication of

deepfake content. Since women make up the majority of those who fall victim to deepfake material, they are frequently the target of publications that publish non-consensual sexual content or any other type of deepfake content with the intention of harming or embarrassing them. It is imperative that these social media platforms maintain their integrity as a secure space for leisure for all users.[15] In order to facilitate users' ability to confirm the legitimacy of the media they come across, social media platforms ought to prioritise transparency in the content generation process. This could entail employing third-party validation tools for media integrity, watermarking, or other certification forms.[16]

[15] Srishty Dey, *Ethical and Legal Challenges of Deepfakes – An Indian Perspective,* III IJLSI 951-968 (2021).
[16] Neill Jacobson, 'Deepfakes and Their Impact on Society' (*CPI OpenFox*, 26 February 2024) <https://www.openfox.com/deepfakes-and-their-impact-on-society/> accessed 10 February 2025.

Quantum Technological Era: Legal Shifts and Challenges

-Nishita Sharma*

Abstract

The year 2025, declared the International Year of Quantum Science and Technology, by the United Nations General Assembly, marks a century since German theoretical physicist, Werner Heisenberg first introduced the foundational theory of quantum mechanics. This symbolic milestone coincides with unprecedented global advancements in quantum technologies, ranging from quantum computing to quantum communication, heralding what is often referred to as the 'second quantum revolution". As tech giants and nation-states alike race to secure dominance in this transformative field based on their priorities, massive investments and national strategies are being rolled out to position themselves as quantum superpowers.

Amidst this surge of technological ambition, the legal and regulatory challenges posed by quantum technologies have yet to be fully conceptualised, let alone addressed. Existing legal frameworks, particularly in areas such as data protection, intellectual property and cybersecurity, are largely unequipped to handle the complex implications of quantum capabilities. The disruptive potential of quantum computing to undermine current encryption standards, for instance, calls for urgent re-evaluation of global data security norms.

This paper explored the foundational principles of quantum mechanics that underpin emerging technologies, maps out major governmental and corporate initiatives driving the quantum agenda, and critically assesses the regulatory gaps that exist in anticipation of this shift. It also evaluates India's position within the global quantum landscape, examining recent national missions, institutional capacities, and policy responses. By adopting an interdisciplinary lens, this paper aims to contribute to the growing discourse on the legal preparedness needed in the face of quantum disruption.

I. Introduction

The rapid advancement in development of quantum computing, represents unparalleled challenges and huge scopes of advanced technologies. As we might already know, quantum physics is one of the most interesting branches of physics, and also one of the most less-understood one. There are numerous unique characteristics of quantum algorithms and hardware, and owing to this there are very different set of problems arising.

Quantum technologies represent a paradigm shift in computing, cryptography, and sensing, challenging existing legal frameworks

* 4th-year student at NALSAR, University of Law.

designed for classical systems[17]. These technologies leverage quantum mechanical phenomena like superposition and entanglement to perform calculations and transmit information in fundamentally different ways than conventional systems. Due to this innovation, there are different needs to establish new frameworks or modify the current ones, focusing on intellectual property, data security, regulations and also ethical considerations.

The legal system faces several challenges in addressing quantum technologies. First, quantum computing threatens current encryption standards, potentially rendering sensitive data vulnerable and undermining privacy laws and cybersecurity regulations. Second, quantum sensing technologies raise novel privacy concerns by potentially detecting information through barriers previously considered impenetrable. International governance presents another challenge, as quantum technologies could disrupt power balances in cybersecurity and intelligence gathering. Export controls and technology transfer regulations require reconsideration in light of these unlimited quantum capabilities. Legal frameworks need adaptation in several key areas. Cryptographic regulations must evolve to establish quantum-resistant standards and transition protocols.

Data protection laws require updating, in order to effectively address quantum-specific vulnerabilities, since there are already multiple plans and frameworks across different jurisdictions contributing to development of the technologies.

In terms of ethical considerations, there are different dimensions that will have to be looked at. As the systems become more powerful, they will pervade important walks of lives, and it would also have profound societal impacts[18], such as exacerbating inequalities, enabling mass surveillance or making the decision-making process automated, as we saw with the rise of AI. Hence, the emphasis should also be on implementing robust ethical guidelines for responsible use of such technologies.

National security frameworks need provisions for quantum communication channels and computing resources. International agreements on quantum technology development and deployment are necessary to prevent fragmented regulations and security vulnerabilities. The legal system must adopt a proactive and flexible approach, incorporating technical expertise in quantum physics while maintaining foundational legal principles of privacy, security, and fairness.

---

[17] John Preskill 'Qauntum Computing in the NISQ era and beyond' (2018) <https://doi.org/10.22331/q-2018-08-06-79> Quantum 2, 79, accessed 12 March 2025.

[18] P. E. Vermaas, 'The societal impact of the emerging quantum technologies: a renewed urgency to make quantum theory understandable' (2017) Ethics and Information Technolgy <https://link.springer.com/article/10.1007/s10676-017-9429-1>.

II. Foundational Theory of Quantum Computing

The evolution of quantum technology can be traced back to the early 20th century, with the rising study of quantum mechanics. However, more practical applications emerged in the late 20th and early 21st centuries. Interestingly, in 2023 the Nobel Prize in Physics was awarded to 3 Quantum physicists.

In 1981, the prominent physicist, Richard Feynman proposed the idea of quantum computers. This served as the bed rock for the 1994 quantum algorithm designed by Peter Shor[19], it demonstrated the potential of quantum computing to break the widely used schemes in encryption.

By 2020, several tech giants like IBM, Google and Intel had developed Quantum computers capable of performing tasks on a much-advanced level than the classical computers. IBM's quantum processor achieved quantum volume milestones[20].

Quantum computing operates on fundamentally different principles than classical computing. It leverages the unique properties of quantum mechanics, specifically, the interactions of subatomic particles such as protons, neutrons, and electrons, to achieve exponentially greater processing power.

Traditional computers rely on binary "bits," which exist in one of two states, 0 or 1, and perform logical operations such as "and," "not," and "or" to process data. They employ a series of circuits, called 'gates', and perform all the logical operations, based on the state of those switches. In contrast, quantum computers substitute the binary 'bits' with "qubits". Qubits operate through the phenomenon of Quantum Superposition, and can exist as 0, 1, or both simultaneously.

Mathematically, superposition equation is a combination of '0' and '1' and is written linearly as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Here, $|\psi\rangle$ is the state of the qubit, and $|0\rangle$ and $|1\rangle$ are the basis states and α and β, are complex numbers called 'probability amplitudes'. These amplitudes determine the probability of measuring the qubit in either state when a measurement is made[21]. This ability enables quantum systems

---

[19] Peter W. Shor, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', (1996) <https://arxiv.org/pdf/quant-ph/9508027> accessed 12 March 2025.

[20] Ankit Singh, "The Impact of Quantum Technology on Data Security" (29 May 2024) <https://www.azoquantum.com/Article.aspx?ArticleID=524> accessed 20 March ch 2025.

[21] Microsoft, 'Explore Quantum Superposition' < https://quantum.microsoft.com/en-us/insights/education/concepts/superposition> accessed 12 March 2025.

to perform multiple calculations at once, significantly enhancing computational efficiency.

Another, reason behind these technologies being extremely rapid, is the phenomenon of 'Quantum Entanglement.' Quantum entanglement is the state where multiple objects- let's say electrons and photons, share a single quantum state[22]. The qubits, can exhibit "entanglement," where the state of one qubit is intrinsically connected to another, regardless of distance. This, in strict quantum physics terms was termed as "spooky action at a distance", by Einstein. The entangled entities, cannot be described as independent anymore.

In quantum computing, this phenomenon of entanglement, allows quantum parallelism. It is the ability of the computer to perform multiple calculations simultaneously. Essentially, it means that many qubits would be entangled in a single operation, and if a measurement is made on one of them and it is $|0\rangle$, the state of the other qubit will immediately collapse to $|0\rangle$ as well[23].

As more qubits become entangled, computational capacity grows exponentially. For instance, in 2019, a 72-qubit quantum computer executed a complex calculation in just 200 seconds, a task that would have taken the most advanced supercomputer an estimated 10,000 years to complete[24].

In 2020, as per a report by McKinsey, by 2030 there would be 2000-5000 quantum computers that would be operational[25].

III. How Do They Differ Significantly From Classical Computers?

Classical computers have been the dominant form of computing for decades. They work by employing binary bits which are in the states of either 0 or 1. This limit them to perform N number of calculations, when N number of bits are employed. However, with Quantum computers they can do 2^N calculations in the same time. If classical computer can do 5 calculations, then a quantum computer can do 32 calculations in the same time.

---

[22] Dan Garisto, ' What is Quantum Entanglement' (8 June 2022) <https://spectrum.ieee.org/what-is-quantum-entanglement> accessed 12 March 2025.

[23] Microsoft, 'Explore Quantum Entanglement' <https://quantum.microsoft.com/en-us/insights/education/concepts/entanglement> accessed 10 March 2025.

[24] Berkeley Nucleonics Corp, "Quantum Computing v Classical Computing" (23 August 2024) <https://www.berkeleynucleonics.com/Augustust-23-2024-quantum-computing-vs-classical-computing> accessed 10 March 2025.

[25] McKinsey Quarterly, "A game plan for Quantum Computing" (6 February 2020) <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing> accessed 13 March 2025.

Quantum computing relies on quantum bits (called qubits), instead of the traditional binary bits. Quantum computing relies on quantum entanglement, essentially what it means is that multiple qubits are sustained in 'quantum-coherent' state, whereby qubits are entangled. In 2024, it was ascertained that fifty qubits was the approximate number where quantum computing becomes capable of calculations very swiftly[26].

Additionally, both types of computers employ algorithms to perform calculations. An input goes in and then the algorithm processes it and puts out an output. Quantum computations[27] take into account multiple options simultaneously and the execution of algorithms take just one step, that too in a very miniscule amount of time. In contrast, classical computers, algorithms take a lot of parallel computations which is very time consuming. Additionally, classical computers also rely on a deterministic algorithm, this means that the output for an input will always remain same, however, quantum computers employ probabilistic algorithms, meaning they can produce a range of outputs, all probabilistic. This entails solving problems that are intractable for the classical computers[28].

IV. Where Can Quantum Computing Be Used

As already described above, the quantum computers excel at handling highly complex operations. They have several potential advantages over classical computing, making them particularly effective for tasks such as simulating particle interactions, solving optimization problems with multiple variables, significantly enhancing AI training processes, and rapidly factoring prime numbers, which an essential aspect of modern encryption systems.

The most notorious of these domains is the use of cryptography. In 1994, mathematician Peter Shor, described quantum computers to pose a significant threat to the traditional security systems[29]. He also

---

[26] Quantropi, ' Quantum Versus Classical Computing and the Quantum Threat' <https://www.quantropi.com/quantum-versus-classical-computing-and-the-quantum-threat/#:~:text=Quantum%20Versus%20Classical%20Computing,-In%20general%2C%20classical&text=In%20classical%20computers%2C%20an%20algorithm,options%20in%20a%20single%20step> accessed 30 March 2025.

[27] Yudong Cao, 'Quantum Chemistry in the age of quantum computing' (2019) Chem.Rev. <https://doi.org/10.1021/acs.chemrev.8b00803> accessed 20 March 2025.

[28] Y Huang and S Pang, "Optimization of a Probabilistic Quantum Search Algorithm with a Priori Information" (2023) 108(2) Physical Review <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.108.022417> accessed 20 March 2025.

[29] Josh Schneider & Ian Smalley, "What is Quantum Cryptography" (1 December 2023) <https://www.ibm.com/think/topics/quantum-cryptography> accessed 10 March 2025.

demonstrated a theoretical quantum computer's ability to effortlessly decipher the encryption algorithm, public key encryption (PKE).

Quantum computers are believed to be capable of breaking many existing encryption schemes. In theory, it is more secure than any of the previous types of cryptographic algorithms and is also unhack-able. Since, it is impossible to predict the exact quantum state of the qubits, they can exist in several positions at any given time, hacking becomes almost impossible without altering the algorithm altogether.

Another area is simulation of complex quantum systems such as molecules, this would allow computers to accurately simulate chemical reactions. It would also consequentially allow for discovering of new materials. These advanced capabilities position quantum computing as a game-changer across various industries, including pharmaceuticals for drug discovery.

V. Current Developments

Scholars term this era as "Second Quantum Revolution" after the first revolution in the early twentieth century. Governments worldwide are making substantial investments in quantum computing research and development, recognizing its transformative potential. The European Union's Digital Decade Strategy aimed for Europe to have its first supercomputer with Quantum Acceleration in 2025, and to have it at the cutting edge of Quantum capabilities by 2030[30].

The European Union has spearheaded several initiatives in this direction, including the Quantum Technologies Flagship, which was launched in 2018. It is a decade-long, €1 billion research and innovation program[31]. In October 2022, the European High Performance Computing Joint Undertaking, (EuroHPC JU), announced six places to have first European Quantum Computers. Alongside these, there is also the European Quantum Communication Infrastructure (EuroQCI), which aims to establish a secure quantum communication network across all 27 EU Member States.[32].

---

[30] European Commission, "Europe's Digital Decemberade : Digital Targets for 2030" <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-Decemberade-digital-targets-2030_en>

[31] European Parliament, "Quantum : What is it and where does EU stand", (10 April 2024) <https://epthinktank.eu/2024/04/10/quantum-what-is-it-and-where-does-the-eu-stand/> accessed 12 March 2025.

[32] Defence Industry and Space, "Quantum Technologies" <https://defence-industry-space.ec.europa.eu/eu-space/research-development-and-inNovemberation/quantum-technologies_en#:~:text=The%20Quantum%20initiative%20%E2%80%9CEuroQCI%20%E2%80%9D%20intends,critical%20infrastructures%20across%20the%20Union> accessed 10 March 2025.

Apart from Europe, China's 14th five-year plan (2021-2025)[33] also provided valuable insights into the country's stance on quantum technologies. According to that, China has become a pioneer in building Quantum communication infrastructure, and that is also its strategic priority in terms of strengthening its national defence and proliferation of economic growth.

In 2018, the US released its National Quantum Strategy and entailed an approach at federal level to improve research and development in Quantum Technology for the same reasons as China. The US also has the National Quantum Initiative Act, which was signed into law in 2018, it established a framework to accelerate quantum research and development. In the United States, the National Institute of Standards and Technology (NIST) has initiated a process to develop and standardize encryption protocols capable of withstanding quantum computing threats, which is about developing new algorithms that are resistant to hacking.

VI. 2025: The year of Quantum Science

The year 2025 marks the centenary of Heisenberg's developments of matrix mechanics, which was the first solidification of the ideas of quantum mechanics into a coherent physical theory. And the United Nations General Assembly also declared 2025 to be the International Year of Quantum Science and Technology (IYoQST), on June 7th, 2024[34].

This worldwide initiative recognizes and celebrates the contributions of quantum science to technological progress since the first formalization of theory by Heisenberg. Quantum theory has revolutionised modern electronics, and is also an important pillar of global telecommunications.

It is also to raise global awareness about the importance of quantum technologies for sustainable development in the 21st century. One of the other important aims is also to ensure that all nations have access to quantum education and opportunities in developing those as well. It also stresses on providing youth, girls and women particularly in developing countries with opportunities of learning about science and technology. The focus on inclusivity and support, is critical, it acknowledges the importance of quantum technologies, and also emphasizes on equitable and diverse perspectives in governance frameworks[35].

---

[33] The Government of Fujian Province, "Outline of the Five-Year Plan (2021-2025) for Social Development and Visions 2035 of the People's Republic of China (9 August 2021) <https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm#C4> accessed 13 March 2025.

[34] UNESCO, "International Year of Quantum Science and Technology"< https://www.unesco.org/en/years/quantum-science-technology> accessed 3 March 2025.

[35] U Gasser, R Budish and S West, "Multistakeholder as Governance Groups: Observations from Case Studies" (2015) Berkman Center Research Publication.

This is also an acknowledgment of increasing transformative power of quantum technologies and their governance requirements. Quantum science and technology is poised to help address the current most pressing challenges, including but not limited to rapidly develop renewable energy, human health in terms of finding more drugs, climate action, clean water and energy, food security. UN stressed on its importance in supporting UN's Sustainable Development Goals[36].

The IYoQST resolution laid the groundwork for developing a governance framework that is inclusive, adaptive, anticipatory, responsive, and harbours diverse perspectives therein. We are in 2025, which is the International Year of Quantum Science and Technology, is an important opportunity for our global community to reap benefits of it and advance towards a more coherent and substantive governance. The emphasis should be on, letting the quantum technologies reach their full transformative promise while limiting the risks and harms posed by this.

This could be done in a lot of ways, particularly ensuring that all of the developments are grounded in Responsible Research and Innovation (RRI). RRI focuses on the importance of anticipating and mitigating the potential risks poses by technologies, while still ensuring that the development and deployment of such technologies is not thwarted[37]. Another possible way is to involve establishment of dedicated quantum technology assessment bodies, and integrating scientific minds and quantum considerations into the existing technological regulation frameworks. Legal professionals must also develop expertise in quantum communication systems, particularly Quantum Key Distribution (QKD), which offers unprecedented opportunities for secure data transmission (Scarani et al., 2009).

As these technologies gain traction, lawyers must be prepared to advise clients on the legal implications of quantum-based security solutions and their role in enhancing data protection. This requires continuous engagement with industry advancements, collaboration with quantum technology specialists, and active participation in relevant legal and technological forums.

---

[36] IUPAC, "The International Year of Quantum Science and Technology" (3 October 2024) <https://iupac.org/the-international-year-of-quantum-science-and-technology-2025/> accessed 2 March 2025.

[37] European Commission, Directorate-General for Communications Networks and Content Technology, Ethics Guidelines for Trustworthy AI (Brussels, Publications Office 2019).

VII. Effect on The Current Encryption Methods

The advent of quantum technologies poses a significant challenge to existing cybersecurity frameworks. As quantum computing has the potential to break widely used encryption methods, rendering traditional data protection mechanisms ineffective, the threat to cybersecurity is imminent[38].

Although, most of it is limited to theoretical reality, this concern prompted the National Institute of Standards and Technology (NIST), to call for development of 'quantum-safe' encryption algorithms. Interestingly, in 2015 the National Security Agency advised the US agencies and businesses to prepare in time, for the 'not-too-distant' future of quantum technologies wreaking havoc on all existing digital realms[39]. It is pertinent to note that, at the time, the time frame for this was approximately 10 years, and now we are in the timeline of this advisory.

The security of the current modern digital communications and transactions, is heavily reliant on the public-key cryptography. It uses mathematical algorithms to encode and decode sensitive information, the most widely used such algorithm is ECC (elliptic curve cryptography). Similar algorithms have been considered secure due to the sheer impossibility of the ability to find efficient solutions to the underlying mathematical problem, because of factoring of large numbers. It is deemed impossible for the classical computers, however, as already mentioned above, the situation significantly changes when quantum computing is considered due to their ability to do such computations easily and efficiently.

The ability of quantum computers to employ phenomena of superposition and entanglement, make it feasible for them to calculate something that is considered relatively impossible for the classical computers. Importantly, we currently lack large scale, quantum computers capable of running the Shor's algorithm, however, given the pace of advancement in the area, it is just a matter of a few years till it is a reality, as per experts.

This would have a devastating effect on the digital systems, this algorithm could be leveraged to break the existing encryption protected data, transferred or stored in digital systems, including financial records and government secrets. One may be inclined to think that this threat is not imminent, then why should we pay attention to it. However, the danger of

---

[38] James Dargan, "Quantum Cybersecurity Explained : Comprehensive Guide" (13 March 2024) <https://thequantuminsider.com/2024/03/13/quantum-cybersecurity-explained-comprehensive-guide/> accessed 10 March 2025.

[39] Dan Goodin, "NSA preps quantum-resistant algorithms to head off crypto-apocalypse", (21 August 2015) <https://arstechnica.com/information-technology/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/> accessed 15 March 2025.

quantum computing is not limited to imminent data breaches, rather, data can be encrypted and saved right now, and can be later decrypted using such quantum computing technologies. Among cybersecurity experts this is the rise of "harvest now, decrypt later" attacks, where malicious actors intercept and store encrypted data today, anticipating the future availability of quantum computers capable of breaking asymmetric encryption. Without pre-emptive quantum-resistant safeguards, businesses could face substantial legal and financial liabilities years down the line.

This has also led to evolution of a field called "post-quantum cryptography"[40] (PQC), which is also called quantum-resistant encryption. PQC is supposed to be resistant to quantum attacks while still retaining the desirable properties of the existing cryptographic systems.

VIII. Data Security and Regulatory Frameworks

The emergence of quantum technologies marks a significant shift in the technological landscape, with profound implications for various sectors, including law. **In 2013, the infamous Yahoo Data Breach[41], where three billion accounts were hacked, then the Aadhaar case in 2018[42] and the Alibaba data breach in 2019[43],** all of these, detail the turmoil that can occur in the digital world. In the growing quantum world, it is imperative to say that they have the potential to compromise the preexisting encryption methods attributed to their advanced computational abilities.

As quantum computing, quantum communication, and related innovations progress at an unprecedented pace, they present novel legal challenges that necessitate the evolution of regulatory and intellectual property frameworks. The intersection of quantum technologies and the law has given rise to an emerging field known as quantum law, which seeks to address these complex issues. Given their potential to disrupt industries ranging from cybersecurity to artificial intelligence, quantum technologies demand careful legal scrutiny to ensure robust governance and protection of rights.

---

[40] National Institute of Standards and Technology, 'Post Quantum Cryptography' <https://csrc.nist.gov/projects/post-quantum-cryptography> accessed 12 February 2025.

[41] Nicole Perlroth, 'All 3 Billion Yahoo Accounts Were Affected by 2013 Attack', *The New York Times* (3 October 2017).

[42] Mardav Jain, 'The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment'(University of Washington News, 9 May 2019) <https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/> accessed 13 February 2025.

[43] Dashveenjit Kaur, 'Is Alibaba responsible for the largest data heist in China' (*Tech Wire Asia,* 18 July 2022) <https://techwireasia.com/2022/07/is-alibaba-responsible-for-the-largest-data-heist-in-china/> accessed 10 February 2025.

IX. The Regulatory Demand to Shift

This shift from classical to quantum technology era, raises urgent concerns about privacy and security, particularly in light of established regulatory frameworks such as the United States' Electronic Communications Privacy Act (ECPA) and the European Union's General Data Protection Regulation (GDPR), which may prove inadequate in addressing quantum-related threats (Smith, 2020).

While these current laws, set out certain basic requirements for appropriate and secure processing, as well as storage of personal data, still these fall short of addressing the problems posed by use of quantum technologies. Policymakers and legal experts must now grapple with the necessity of updating these regulations to account for the unprecedented risks posed by quantum advancements[44].

Furthermore, the intellectual property landscape faces new complexities, as quantum innovations give rise to novel challenges in patenting, licensing, trade secrets, and other forms of IP protection, necessitating a re-evaluation of existing legal doctrines to accommodate this rapidly evolving field.

X. The Current Regulatory Frameworks

The rapid evolution of quantum technologies demands a proactive legal approach to address emerging challenges effectively. The disruptive potential of quantum computing presents significant legal challenges that must be addressed proactively. One of the most urgent concerns is the profound impact quantum advancements could have on cryptography and digital security.

Many of today's encryption protocols, including RSA and elliptic curve cryptography, are based on mathematical problems—such as prime factorization and discrete logarithms—that classical computers struggle to solve. However, Peter Shor's groundbreaking quantum algorithm (1994) demonstrates that a sufficiently powerful quantum computer could efficiently solve these problems, rendering conventional encryption methods obsolete and compromising the confidentiality of encrypted data.

This looming threat underscores the necessity of developing and implementing quantum-resistant or post-quantum cryptographic solutions. Governments, businesses, and legal institutions must prepare for a post-quantum security landscape by fostering research, updating

[44] Mauritz Kop, 'Towards Responsible Quantum Technology' (21 March 2023) Harvard Berkman Klein Center for Internet and Society Research <https://cyber.harvard.edu/publication/2023/towards-responsible-quantum-technology> accessed 30 March 2025.

regulatory frameworks, and ensuring the seamless transition to encryption standards resilient to quantum attacks.

As with any groundbreaking technology, quantum computing is likely to fuel a surge in legal disputes. Its capacity to significantly enhance artificial intelligence and machine learning could amplify existing concerns over algorithmic bias and flawed decision-making, leading to litigation over unfair or harmful outcomes.

As already developed throughout the paper, the major source of contention will be quantum computing's ability to crack current encryption methods, potentially exposing sensitive personal, financial, and commercial data to cybercriminals. This risk could trigger waves of negligence-based class actions from affected consumers, commercial disputes between businesses, and even shareholder litigation over the financial impact of a data breach. Regulators worldwide are already exploring ways to "quantum-proof" cybersecurity, and companies that fail to take proactive steps may find themselves facing legal action from various stakeholders[45].

From a legal standpoint, current privacy and cybersecurity frameworks are built around the principle of "reasonable security," meaning businesses must implement protective measures that align with the prevailing threat landscape. However, as quantum computing advances toward mainstream adoption, the legal interpretation of what constitutes "reasonable" security may evolve.

The current data protection laws like GDPR and California Consumer Privacy Act[46], would have the locus for regulation of certain aspects of quantum technologies, like cybersecurity and data protection, but they would need significant tailoring bespoke for quantum technologies. For instance, the GDPR mandates that data controllers implement "state-of-the-art" security measures, but such protections may become obsolete if quantum computing renders traditional encryption ineffective. If quantum computers render public encryption keys obsolete, the consequences could be catastrophic for digital ecosystems.

The synergy between quantum hardware and software is critical for implementing these algorithms. Quantum hardware, including superconducting qubits and ion traps, forms the foundation of quantum computation, while quantum programming languages and compilers translate abstract quantum algorithms into executable instructions. Frameworks like Qiskit, OpenQASM, and Q# facilitate the development and optimization of quantum algorithms for specific hardware

[45] : K Balarabe, "Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap" EJRR <https://doi.org/10.1017/err.2025.8> accessed 15 March 2025.
[46] California Consumer Privacy Act (CCPA) <https://oag.ca.gov/privacy/ccpa> accessed 15 March 2025.

architectures. This dynamic interaction between quantum hardware, software, and algorithms is fundamental to realizing the full potential of quantum computing.

Thus, Quantum technologies are expected to be safeguarded through a combination of intellectual property (IP) protections, given their complex structure and multidisciplinary nature. A quantum computer comprises various components, including qubits, quantum gates, multipliers, chips, processors, and cooling systems, alongside the software that enables their functionality. Thus, even patent laws and intellectual property rights have a major role to play in the regulation of quantum technologies.

Patent law, which protects novel, useful, and non-obvious human inventions, is particularly relevant for securing advancements in quantum hardware. Meanwhile, copyright—requiring originality, creativity, and human authorship—is better suited for software-related aspects of quantum computing. Quantum algorithms, often open source in nature, can be eligible for copyright protection once converted into source code. Additionally, patents may apply to certain algorithmic applications that produce a technical effect on quantum hardware. Since quantum computing outputs typically involve human intervention at some stage, they may also be considered intellectual property, akin to traditional software-generated content.

National security concerns surrounding quantum computing could lead to stricter regulations, with some quantum technologies potentially being classified as state secrets. Furthermore, ongoing debates in academic and policy circles question whether traditional IP protections, such as copyright extending for the life of the author plus 70 years, are being considered too rigid for such a rapidly evolving field.

While the stage of development for quantum technologies is still nascent, various international organizations like the World Economic Forum and OECD, and some governments like the US, the UK, Germany, and Japan, have already initiated efforts to address the possible governance challenges posed by these rapidly emerging technologies. The European Commission has introduced proposals aimed at adapting IP frameworks to better accommodate advances in data science and artificial intelligence, signalling potential shifts in how quantum innovations will be protected in the future.

XI. Comparative Analysis: Different Frameworks

To date, different jurisdictions have their own approaches towards developing regulatory mechanisms for quantum technologies. It depends on national priorities, standards, and levels of technological capabilities and existing policy frameworks.

In the US, the National Quantum Initiative Act, was signed into law in 2018. It established a nationally coordinated programme to accelerate quantum research and development, and also allowed for effective public-private partnerships which would contribute to qualified quantum workforce[47]. It also sought to direct the federal governments in their investments in quantum technologies, including consideration of dimensions like legal, ethical and wider societal.

Europe has been a pioneer in this area, it recognized the inevitable strategic importance of quantum technologies, thereby launching several initiatives to support developments as well as regulations to assure minimal damage. European Commission called for a coordinated approach to quantum regulation, and asked for development of European Quantum Policy. This was to ensure that there remains a coherent framework for the development and governance of such emerging quantum technologies, within the European Union. Further, the €1 EU Quantum Flagship, which was launched in 2018 aimed to consolidate and expand the European leadership in this field. This initiative also explicitly addressed quantum technologies, and their societal and ethical implications.

China is also a big contender in quantum era. Its pursuit of quantum technology has been more state led, with a lot of government funds and dialogue facilitations between the public and private sectors. As mentioned previously, the regulations on quantum technologies are based on numerous factors, and, for China it is about situating the country at the forefront of quantum developments. There, quantum technology is a national priority and huge investments are made in research and development. China aims to make substantial and real breakthroughs by as close as 2030. Till 2022, the total investments in quantum technologies in China was $15.3 billion that culminated in a National Quantum Program, this is more than the US and EU cumulatively. China's Educational Modernisation 2035 Plan also emphasizes on quantum technology in the education sector. It also has a somewhat less robust regulatory framework for quantum technologies, which more or less focuses on making as many technological advancements in the quantum sector as rapidly as possible, and putting in place security measures for it.

India is also taking steps towards it. In April 2023, India launched the National Quantum Mission which is to be implemented till 2031 by the Department of Science and Technology. It had four areas: Quantum Computing, Quantum Communication, Quantum Sensing and Metrology and lastly, Quantum Materials and Devices.

[47] National Quantum Initiative Act [2018] H.R.6227.

Similarly, other countries such as Canada[48]., Japan[49] and Australia[50] have also launched numerous national initiatives to strategize and develop quantum technologies, with varying degrees of emphasis on its regulation, based on what they deem important

XII. Ethical Dimensions

It is also pertinent to identify the potential ethical problems that would emerge with quantum technologies. Since, it is set to completely revolutionize the technological arena, it would inevitably have a lot of ethical implications. By focusing on the ethical dimensions, we can not only allow exploitation of social values of technologies but also, find solutions for risk management from all perspectives.

One argument that keeps being iterated is that, quantum technologies is a nascent technology, its development has largely limited itself to theoretical dimensions, and it is often influenced by a strong rhetoric of revolutionising the future of technologies. However, quantum technologies can be used as an umbrella term for all such range of technologies that are emerging, which are very different from each other but have very strong impacts in all dimensions.

Interestingly, while there are so many discussions and discourse around quantum regulations and strategies, there is no focus on specific ethical problems. In the UK and EU, midterm report on quantum strategy, the terms like 'ethics", and 'morals' did not appear. Some important facets of this discussion are also that there would be a huge imbalance between populations with advanced quantum technologies and the ones without it. As already explained, there would be a new definition of privacy in quantum age, given encryption would be changed drastically.

Additionally, in 2022, the US National Security Memorandum published a report that stated that in order to cope with the risk poses by quantum cryptography, it must promote collaborations with overseas allies, in education and professional aspects. This international engagement would

---

[48] Government of Canada, "Canada's National Quantum Strategy" (Government of Canada, 2 February 2020) <https://ised-isde.canada.ca/site/national-quantum-strategy/sites/default/files/attachments/2022/NQS-SQN-eng.pdf > accessed 22 March 2025.

[49] The Government of Japan, Touching the cutting edge of quantum technology in the homeland of the superconducting qubit (31 May 2022) <https://www.japan.go.jp/kizuna/2022/05/cutting_edge_of_quantum_technology.html > accessed 20 March 2025.

[50] Australian Government, "National Quantum Strategy" (2 May 2023) <https://www.industry.gov.au/sites/default/files/2023-05/national-quantum-strategy.pdf> accessed 20 March 2025.

prove to be essential in identifying various risks and inculcating diverse perspectives on quantum security and protection[51].

One of the key points in discussions about ethical implications of quantum technologies, revolve around social issues concerning equity, diversity and inclusion specifically for marginalized groups in academic literature, policy and debates on quantum technologies. It has been a normal way of looking at technological advancements purely from a legal perspective, and rarely an eye is turned towards the 'social' of it.

One way around it is to inculcate RRI as already described above. RRI helps facilitate public dialogues, envisages involvement of parliaments, allows from inputs from all relevant stakeholder, and given the stochastic nature of the quantum computational system, it is important to have a transparent process. Given that quantum computing inculcates quantum physics which is notoriously misunderstood and less-understood, the need for transparency in communication, explanation and interpretation of quantum algorithms becomes pertinent[52].

Quantum cryptography is the most notorious area of all of it, and cryptography is also an indispensable means to protect information in a computer system. Peter Shor in 1994 already showed that quantum computer can easily solve several of the computational problems. This essentially meant that anyone with a real-world quantum computer would be capable of easily breaking the cryptographic codes, thus compromising the encrypted communications.

At the conjuncture of this problem is the ethical dimension of security v privacy. One way to potentially deal with it is to cultivate post-quantum algorithms like lattice systems, coding-based systems etc. This would raise questions of governmental paternalism, and diminishing rights of privacy and autonomy.

The interplay between ethics and law is crucial in shaping regulations that govern quantum technologies. Legal frameworks must incorporate ethical principles to ensure accountability, prevent misuse, and promote transparency in quantum-powered systems. The ever-impending question of privacy and autonomy will always loom over us, and the key is to find a good balance between them in an ever-changing and rapidly advancing technological ground.

---

[51] Scott Buchholz & Beena Ammanath, 'Quantum computing May create ethical risks for businesses' (*Deloitte Insights,*12 May 2022) <https://www2.deloitte.com/us/en/insights/topics/cyber-risk/quantum-computing-ethics-risks.html> accessed 18 March 2025.

[52] Luca M. Possati, 'Ethics of Quantum Computing' [2023], Vol. 36 Philosophy and Technology <https://link.springer.com/article/10.1007/s13347-023-00651-6> accessed 19 March 2025.

XIII. Where does India Stand on All of this

On 19th April, 2023, India approved the National Quantum Mission (NQM), which envisioned propelling India into the international forefront of quantum technology research and development. It has a budgetary allocation of Rs. 6,000 crores for the period of 2023-2031. With this, India aims to harness the power of quantum technology to drive innovation in the field and also to position itself as a global leader in this cutting-edge field.

Many countries are already working on this in a more proactive way, making significant contributions to the field, like the US, EU, and China. Since, quantum technology will percolate the most important walks of life like healthcare, clean energy, climate change, data and cyber security, India has a chance to play a key role in the regulatory framework.

As a part of this mission, a total of four Thematic Hubs has been chosen (T-hubs)[53], these bring together 14 Technical groups across 17 states and 2 Union territories. The focus will be on technology innovation, skill development, industry partnerships, fostering a global collaborative space to ensure a national impact. An important feature of these T-hubs is that, they will work on a Hub-Spoke-Spike Model which will foster a cluster-based network. It will focus on a collaborative ecosystem involving 152 researchers from 43 different institutions across the country[54].

Further, India's journey towards becoming a global leader in quantum technology also involves strategic investments. One such initiative to bridge the gap between research and industry is Quantum Computing Applications Lab, which is led by the Ministry of Electronics and Information technology. This lab supports India's aspirations to create a thriving quantum research hub.

Another important step is equipping India's academic institutions to evolve research in quantum technologies. This flows from "Jai Anusandhan" vision of the government, wherein they work closely with the Department of Telecommunications and Department of Science and Technology[55].

Thus, in a nutshell, India's advancements in quantum computing represent a coordinated effort between various stakeholders, including the

---

[53] These are: 1. Quantum Computing, 2. Quantum Communication, 3. Quantum Sensing and Metrology and 4. Quantum Materials and Devices.

[54] Ministry of Science and Technology *National Quantum Mission: India's Quantum Leap* (17 March 2025) <https://pib.gov.in/PressNoteDetails.aspx?NoteId=153963&ModuleId=3&reg=3&lang=1> accessed 18 March 2025.

[55] Cierra Choucair, 'Qauntum Computing in India : Ecosystem Growth & Key Initiatives in 2024' (*Quantum Insider,* 27 November, 2024) <https://thequantuminsider.com/2024/11/27/quantum-computing-advancements-in-india/> accessed 20 March ch 2025.

government, academic scholars, private sectors and evolving startup ecosystem. This has also been a insight of Niti Aayog, which was published in the March 2025 edition of Future Front[56].

XIV. Regulatory Challenges in India

While, India has taken steps towards quantum advancement, it lacks a specific quantum technology regulatory framework. As explained throughout the paper, there is a big threat on current encryption standards, and there is a need to establish a quantum-safe encryption standard.

Given that the other jurisdictions are already ahead of India in this, we can take inspiration from them. In the US, the quantum ecosystem thrives on strong government funding and a dynamic private sector. This is something, the Indian government has already started with the National Quantum Mission. In Europe, there is more emphasis on regional collaboration and strategic autonomy. And in most other jurisdictions the emphasis is also on fostering international dialogues and collaborations.

India must prepare for disruptive breakthroughs, as there are new platforms like silicon spin or topological qubits that have the potential to shorten the quantum timeline, hence, we need to be prepared in advance.

The emphasis should be to foster cooperation between various stakeholders like industry, academia, civil society etc. International cooperation, produce innovation but mitigate risks. Emphasize adaptability.

XV. Conclusion

As we stand at the threshold of a new era in science and technology, the quantum revolution presents both an extraordinary opportunity and a formidable challenge. The year 2025, marking a century since the birth of quantum mechanics, has not only been symbolically recognized by the United Nations, but has also emerged as a watershed moment in global technological development.

Quantum technologies, be it computing, cryptography, sensing or communication, have the potential to reshape the digital landscape in profound and irreversible ways. And so, the critical need to reassess and reimagine existing legal and regulatory frameworks. Quantum computing's capacity to break current cryptographic systems threatens the foundational security structures that underpin global digital

[56] NITI Aayog, *Quantum Computing : National Security Implications & Strategic Preparedness,* Issue 2, (March . 2025).

infrastructure. The legal community must, therefore, move beyond reactive governance and adopt a proactive, anticipatory approach to regulation. This involves creation of flexible, principles-based frameworks that can adopt to the rapid pace of quantum advancements while ensuring accountability, security and ethical integrity.

India's recent push toward quantum leadership through the National Quantum Mission and various public-private collaborations is a promising step in the right direction, yet, for India to emerge as a serious global player, it must also invest in developing legal, ethical and policy ecosystems.

This paper has explored foundations of quantum technology, highlighted major global initiatives, exposed shortcomings in regulations and assessed India's emerging role in this landscape. Ultimately, it has asserted that innovation is not an enemy of the legal, rather the goal is to keep pace with technological change, to shape it responsibly. As we stand at the threshold of a quantum revolution, it is only apt to recall Niels Bohr's timeless words:

"Anyone who is not shocked by quantum theory has not understood it."

Can The First-Ever Registered Case of Virtual Rape Change Legal Standards for Minors in the Metaverse?

- -Anjuli Pandey* and Pallakshi Pandiya**

Abstract

Introduced as a surreal novelty in the world of technology, immersive virtual reality (herein VR) is now a part of life for many through the metaverse. By embodying personas, users can interact with each other within the 3D environment of the Metaverse. Notably, much of the consumer base comprises people below eighteen due to the integration of the virtual world with gaming. However, with every advancement, a new set of challenges arises. In January 2024, a sixteen-year-old girl was gang raped virtually in the metaverse, sending shockwaves throughout the local and virtual community, opening the doors to a one-of-a-kind police investigation. However, this is not the first instance but rather one of many sporadic instances of sexual harassment of women and children in the metaverse. Unfortunately, the ramifications of such experiences include psychological impacts that mirror responses elicited after real-world sexual harassment. The immersive, real-like nature of the metaverse further aggravates it. Consequently, it is becoming increasingly crucial for lawmakers to take cognizance of the fresher challenges that have taken shape due to the increased access to the metaverse. Although the current statutes and directives lack the breadth to encompass metaverse platforms under their ambit, they do possess the potential to form the base for future legislations that define accountability and protect the users. This paper explores the impact of virtual sexual harassment, the existing lacunae in the regulation of sexual harassment in the metaverse, and the scope of improving the security of users, especially minors.

Keywords: *Metaverse, Virtual Reality, Online Sexual Harassment, Minors, Lack of Indian Legal Provisions.*

I. Introduction

The Metaverse is a fully immersive 3D environment that allows users to interact with other users around the globe through avatars in a world that feels almost entirely real. The experience of VR in the Metaverse makes it difficult to separate emotions generated in the virtual world from real emotions. With the Metaverse's emerging role, its problems are also emerging. Developments such as Elon Musk's Neuralink blur the line between the real and virtual world. Along with its mission to build a safe and effective clinical BMI (Brain Machine Interface) system, Neuralink's recent demonstration of a monkey playing the video game Pong with the

* Second year B.A. LL.B. (Hons.) student at Dr. Ram Manohar Lohiya National Law University, Lucknow.
** Second year B.A. LL.B. (Hons.) student at Dr. Ram Manohar Lohiya National Law University, Lucknow.

help of an implanted brain chip reflects the exceptional potential of brain-computer interfaces.[57]

Metaverse platforms have gained worldwide popularity in recent years. As of 2024, the Metaverse has over six hundred million active users worldwide. As per Statista, India is a part of this growing segment. Of these six hundred million, fifty-one % of Metaverse users are thirteen or younger, and eighty % (approximately) are under eighteen.[58] The top applications are currently witnessed in the gaming industry. This increase in the user database has also heightened the issue of sexual abuse in the Metaverse due to the gaps in the current regulatory frameworks. This massive engagement, especially of teenagers, aggravates the necessity of effective legal mechanisms that address the instances of sexual harassment taking place in VR. The Centre for Countering Digital Hate (CCDH) revealed shocking details when the VR Chat, the most reviewed social app in Facebook's VR Metaverse, was filled with abuse, harassment, racism, and pornographic content.[59] Researchers found that users, including minors, face instances of abusive behaviour every seven minutes.[60]

In January 2024, the United Kingdom faced its first-ever registered case of virtual gang rape in the Metaverse, an event that sent shockwaves through the legal and virtual communities alike.[61] A sixteen-year-old girl reported that her avatar- her digital character- was allegedly gang raped by several male avatars while they were engaged in a VR game on a popular Metaverse platform. It was the kind of VR experience that was so vividly presented through a headset that it would severely cause psychological distress akin to actual sexual assault.[62] UK reports of police sprees brought up outrage and questioned the safety of digital environments.

---

[57] Jane Wakefield, 'Elon Musk's Neuralink 'shows monkey playing Pong with mind' (*BBC*, 9 April 2021) <https://www.bbc.com/news/technology-56688812> accessed 10 December 2024.

[58] Naveen Kumar, 'Metaverse Statistics (2025): Active Users Data' (*Demand Sage,* 29 November 2024) <https://www.demandsage.com/metaverse-statistics/> accessed 10 December 2024.

[59] Soyoung Park and Jiwon Kim, 'Fear of Sexual Victimization in Metaverse: A Comparison of Adolescent and Adult Female Users' (2024) 27 Cyberpsychology, Behavior and Social Networking <https://doi.org/10.1089/cyber.2023.0382> accessed 10 December 2024.

[60] 'New research shows Metaverse is not safe for kids' (*Center for Countering Digital Hate*, 30 December 2021) <https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/> accessed 10 December 2024.

[61] 'Virtual gang rape reported in the Metaverse; probe underway' *The Hindu* (04 January 2024) <https://www.thehindu.com/sci-tech/technology/virtual-gang-rape-reported-in-the-metaverse-probe-underway/article67705164.ece> accessed 12 December 2024.

[62] ANI, 'In a first, UK police investigating virtual gang rape of girl's 'avatar' in metaverse' *The Indian Express* (3 January 2024) <https://timesofindia.indiatimes.com/world/uk/in-a-first-uk-police-investigating-virtual-gang-rape-of-girls-avatar-in-metaverse/articleshow/106524371.cms> accessed 12 December 2024.

II. When Avatars Turn Predators: Harassment in the Metaverse

The incident in question is not an isolated one. Instances of sexual harassment are becoming increasingly prevalent in virtual spaces as technology, such as the Metaverse, continues to evolve. A BBC News researcher, posing as a thirteen-year-old girl, witnessed grooming, sexual material, racist insults, and a rape threat in the VR world.[63] The researcher visited VR rooms where avatars were simulating sex. She was shown sex toys and condoms and approached by numerous adult men. One man reportedly told the researcher that avatars could "get naked and do unspeakable things." Others talked about "erotic role-play."

As per the 2024 Statistics, Roblox is the most popular game in the Metaverse and allows children under thirteen to play the game, with over seventy million daily active users. It is one of the most popular games among children in the world.[64] Roblox sex games are commonly referred to on the platform as "condos." They are spaces generated by users where people can talk about sex, and where their avatars can have virtual sex. In these games, Roblox's rules are thrown out the window. The most worrying part is that children and adults may potentially socialise together in these spaces. Much of what is written on chats in condos is unprintable on a grown-up news website, let alone a children's game. Disturbingly, but not surprisingly, a woman claimed to have suffered a virtual sexual assault on the platform.[65]

Not only children but also adults have reportedly experienced sexual harassment in the Metaverse. One of the early examples of this was about a researcher from SumOfUs, who wrote that her avatar was sexually assaulted in Meta's Horizon Worlds.[66] She noted that she was surrounded by male avatars groping her and making sexual innuendos. She described that event as being very psychologically disturbing despite not having any physical contact. The researcher stresses how, even in virtual environments, these assaults can have a significant emotional impact on the victims.

---

[63] Angus Crawford and Tony Smith, 'Metaverse app allows kids into virtual strip clubs' (*BBC*, 23 December 2022) <https://www.bbc.com/news/technology-60415317> accessed 12 December 2024.

[64] Naveen Kumar, 'Metaverse Statistics (2025): Active Users Data' (*Demand Sage*, 29 November 2024) <https://www.demandsage.com/metaverse-statistics/> accessed 12 December 2024.

[65] James Clayton and Jasmin Dyer, 'Roblox: The children's game with a sex problem' (*BBC*, 15 February 2022) <https://www.bbc.com/news/technology-60314572> accessed 13 December 2024.

[66] 'Female avatar sexually assaulted in Meta VR platform, campaigners say' (*BBC*, 25 May 2022) <https://www.bbc.com/news/technology-61573661> accessed 13 December 2024.

Numerous women have since reported unsettling experiences on platforms like Horizon Worlds.[67] Bloomberg's technology columnist Parmy Olson described her experience in the Metaverse as "creepy and uncomfortable" after being crowded by male avatars who took pictures of her.[68] She reported feeling like somebody was speaking in her ear when avatars got too close, as harassment in the Metaverse feels particularly invasive due to the immersive nature of the VR experience.

III. Virtual Scars, Real Tears: Unpacking the Psychological Toll of Metaverse Assaults

In the virtually enveloping digital realm of the metaverse, avatars are disproportionately exposed to acts of sexual abuse and violence. These acts encompass simulated sexual harassment, groping, and assault, among other violations. Despite such instances occurring in a virtual environment with no body-to-body contact between the avatars, their impact on victims profoundly evokes emotional and psychological responses akin to those experienced in the real world. The report *Sexual Violence and Harassment in the Metaverse: A New Manifestation of Gender-Based Harms* highlights the inadequacies in governance and the pervasive threat of sexual harassment in the metaverse.[69]

One of the most alarming facets of harassment in the metaverse is the visceral realism afforded by haptic (tactile) technology and three-dimensional VR environments.[70] Through the use of VR glasses and full-body tracking, interactions in these spaces can translate into real sensations and trigger emotional responses in users. Victims of metaverse assaults often freeze in response to these incidents, unable to remove their VR equipment. This can be attributed to the Proteus effect,[71] which is the tendency for people to be affected by their digital representations, such as

---

[67] Tanya Basu, 'The Metaverse Has a Groping Problem' (2021) MIT Technology Review <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/> accessed 13 December 2024.

[68] Jane Wakefield, 'Meta moves to tackle creepy behavior in virtual reality' (*BBC,* 4 February 2024) <https://www.bbc.com/news/technology-60247542> accessed 13 December 2024.

[69] Carlotta Rigotti and Gianclaudio Malgieri, 'Sexual Violence and Harassment in the Metaverse' (*The Alliance for Universal Digital Rights, Equality Now and The International Observatory on Vulnerable People in Data Protection*, 13 April 2024) <https://audri.org/wp-content/uploads/2024/04/EN-AUDRi-Sexual-violence-and-harassment-in-the-metaverse-03.pdf> accessed 13 December 2024.

[70] Benjamin Schöne and others, 'The Reality of Virtual Reality' (2023) 14 Frontiers in Psychology <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1093014/full> accessed 13 December 2024.

[71] Nick Yee and Jeremy Bailenson, 'The Proteus Effect: The Effect of Transformed Self-Representation on Behavior' (2007) 33 Human Communication Research 271<https://doi.org/10.1111/j.1468-2958.2007.00299> accessed 13 December 2024.

avatars, digital profiles, and social networking personas, i.e., people's behaviour shifts by their digital representations. Consequently, victims may endure psychological harm that mirrors the aftermath of real-world sexual violence. Virtual sexual assault can inflict significant psychological trauma on victims, akin to real-life experiences.[72] The immersive nature of VR exacerbates this trauma, as users perceive the virtual environment as genuine, potentially triggering past traumas for those who have previously endured sexual assault. In an account by a metaverse beta tester who faced a "virtual gang-rape" within minutes of joining Meta's Venues, she voices it as "A horrible experience that happened so fast and before I could even think about putting the safety barrier in place. I froze. It was surreal. It was a nightmare."[73] It led to Meta rolling out a minimum distance between users' avatars in its VR Horizon through the "personal boundary" function.[74]

The immersive nature of social VR aggravates the psychological toll of harassment. Not similar to conventional online media, social VR facilitates personified interactions through features such as full-body tracked avatars, voice communication, body language, and gestures. These features aimed at increasing the blanket feel of the virtual world, in turn, create a heightened sense of presence and realism, which can amplify the emotional distress caused by harassment. In the case of minors, the impact is exponentially heightened, scarring them with a traumatic experience.[75] Haley Kremer, aged fifteen, said she turns to Horizon Worlds to socialize; however, she has encountered stalking by an adult male avatar on the platform. 76 More recently, an under-sixteen minor endured a 'virtual gang rape' on a metaverse platform, prompting a police investigation and highlighting the issue of child safety against sexual offences on an

---

[72] Nishtha Chaudhary, 'AI-Powered Justice: Metaverse Dynamics, Sexual Harassment, Influence of AI on Crime & Legal Protection – Assessing Gaps and Solutions' (*Live Law*, 23 December 2024) <https://www.livelaw.in/lawschool/articles/ai-powered-justice-metaverse-dynamics-sexual-harassment-influence-of-ai-on-crime-legal-protection-assessing-gaps-and-solutions-250671#:~:text=Virtual%20sexual%20assault%20can%20inflict,have%20previously%20endured%20sexual%20assault> accessed 16 December 2024.

[73] Nina Jane Patel, 'Reality or Fiction?' (*Medium*, 21 December 2021) <https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0> accessed 16 December 2024.

[74] Dr. Hassan Elhais, 'A New Frontier for the Law: Navigating Legal Issues in the Metaverse' (*Lexology*, 11 May 2022) <https://www.lexology.com/library/detail.aspx?g=089c80cf-7841-4758-9bb4-a727d46cf905> accessed 16 December 2024.

[75] Michael Hinz, 'Risks the Metaverse Poses for Children and Adolescents: An Exploratory Content Analysis' (*University of Twente Student Thesis*, 2023) <https://essay.utwente.nl/96818/1/Hinz_BA_BMS.pdf> accessed 16 2024.

[76] 'Kids are flocking to Facebook's 'metaverse.' Experts worry predators will follow' *The Washington Post* (7 February 2022) https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/ accessed 19 December 2024.

international scale.[77] It is to be noted that when new online forums arise that attract kids, sexual predators are often among the first to arrive."[78] "They see an environment that is not well protected and does not have clear reporting systems. They'll go there first to take advantage of the fact that it is a safe ground for them to abuse or groom kids." Kids as young as seven years of age face threats of sexual assault on these virtual platforms.[79] Such conspicuous occurrences are especially disquieting when the victims are minors. Research from the Center for Countering Digital Hate (CCDH) found that minors were regularly exposed to graphic sexual content, racist and violent language, bullying, and other forms of harassment on VRChat's platform, which is typically accessed through Meta's Oculus headsets.[80]

Harassment in virtual environments is not a new phenomenon.[81] The infamous 1993 incident of "A Rape in Cyberspace" involved a text-based assault in the LambdaMOO virtual world, which victims reported as emotionally damaging despite its primitive technological context. As online spaces have evolved, the severity and impact of such behaviour have intensified with the advent of sophisticated immersive technologies. Social VR, by moving beyond the 2D screen experience, amplifies the emotional harm associated with harassment, making it an urgent area for intervention. A study showed that harassment, coupled with the immersive VR technology associated with the metaverse, can increase the psychological impact on the user's mental health compared to traditional online spaces. Interviews conducted in the study's ambit indicated that the psychological impact they felt after the harassment took place in VR was greater compared to other online mediums, such as social media.[82] Since

---

[77] Nancy Jo Sales, 'A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future?' *The Guardian* (5 January 2024) <https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta> accessed 19 December 2024.

[78] 'Kids are flocking to Facebook's 'metaverse.' Experts worry predators will follow' *The Washington Post* (7 February 2022) <https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/> accessed 19 December 2024.

[79] Mitchell Van Homrigh, 'Metaverse: Young girls 'virtually raped,' new report reveals' (*news.com.au,* 31 March 2022) <https://www.news.com.au/technology/online/internet/metaverse-young-girls-virtually-raped-new-report-reveals/news-story/c28ceebb2707cf89413c059ee549a2e4> accessed 19 December 2024.

[80] 'New research shows Metaverse is not safe for kids' (*Center for Countering Digital Hate, 30 December 2021)* <https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/> accessed 20 December 2024.

[81] Kelsea Schulenberg and others, '"Creepy Towards My Avatar Body, Creepy Towards My Body": How Women Experience and Manage Harassment Risks in Social Virtual Reality' (*ACM Digital Library*, October 2023) <https://dl.acm.org/doi/pdf/10.1145/3610027> accessed 20 December 2024.

[82] L Blackwell and others, 'Harassment in Social Virtual Reality: Challenges for Platform Governance' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1 <https://dl.acm.org/doi/10.1145/3359202> accessed 21 December 2024.

VR creates the feeling of being physically present in this space, physical altercations or harassment can induce a similar level of realness as in real life.[83]

The void in governance in the metaverse exposes users, particularly women and minors, to harm.[84] Platform providers and governments should focus on the furtherance of safety measures in tandem with today's technological advancements.[85] Additionally, further research is needed to understand the psychological impact of metaverse assaults and to develop effective strategies for prevention and support. In essence, there exists a lacuna of governance and the scourge of sexual harassment in the arena of the metaverse, which detrimentally affects the afflicted users, including children, by exposing them to a heightened probability of being harassed than in the real world.

IV. Laws of the Land, Void in VR: India's Gaps in Protecting Virtual Victims

So far, it has been understood that there is a dire need to bring in sound legal provisions to regulate online sexual predators and limit the harm inflicted upon the victims. Although there exist specific provisions that slightly address the growing issue of online sexual harassment,[86] especially among children, when the talk is about the metaverse, there is a vast vacuum in the system where no explicit rules and regulations exist.

The current definition within our legal framework is narrow, and it mainly covers the harassment taking place in the physical world, ignoring the possibility of the same taking place in the virtual world. One of the current legislations that touches upon the issue of online sexual harassment is Section 66E (punishment for violation of privacy) of the Information and Technology Act (IT Act), 2000.[87] While this provision is aimed at addressing the sexual harassment taking place through online platforms,

---

[83] 'Han and others, 'Virtual Reality Consumer Experience Escapes: Preparing for the Metaverse' (2022) 26(4) Virtual Reality, Research Gate 1443 <https://www.researchgate.net/publication/359253865_Virtual_reality_consumer_experience_escapes_preparing_for_the_metaverse> accessed 23 December 2024.

[84] RR Krishna, 'Challenges in the Metaverse Jurisdiction and International Treaty Law' [2023] 2023 Intergovernmental Research and Policy Journal <https://irpj.euclid.int/articles/challenges-in-the-metaverse-jurisdiction-and-international-treaty-law/> accessed 23 December 2024.

[85] Michael Hinz, 'Risks the Metaverse Poses for Children and Adolescents: An Exploratory Content Analysis' (*University of Twente Student Thesis*, 2023) <https://essay.utwente.nl/96818/1/Hinz_BA_BMS.pdf> accessed 23 2024.

[86] 'Combating the Growing Menace of Online Sexual Exploitation and Abuse of Children in India' (*Child Fund India*, 14 April 2023) <https://childfundindia.org/cf-media/combating-the-growing-menace-of-online-sexual-exploitation-and-abuse-of-children-in-india-indiatimes/> accessed 25 December 2024.

[87] Information and Technology Act 2000, s 66E.

it does not extend to punishing the predators in instances of sexual harassment in the virtual world in VR. Some other specific provisions of the Bhartiya Nyaya Sanhita (BNS) also address sexual instances happening in the online or real world. Section 75 of the BNS[88] describes an act of sexual harassment as something that could only be committed by a man. It negates the possibility of sexual harassment taking place in the virtual world. Moreover, Section 79 of the BNS[89] describes the words, gestures, or acts intended to insult the modesty of a woman. These definitions do not cover the possibility of a woman, a minor, a man, or any human getting molested in a virtual setting. Furthermore, Avatars not being considered an entity that laws can regulate further complicates the possibility of bringing in legislation to punish the molesters.

Additionally, certain other provisions of the IT Act of 2000 are helpful when it comes to addressing the issue of sexual harassment on online platforms: some of these include Section 72 (penalty for breach of confidentiality and privacy),[90] Section 67 (punishment for publishing or transmitting obscene material in electronic form),[91] and Section 67A of the IT Act, 2000[92] (punishment for publishing or transmitting material containing sexually explicit acts, etc., in electronic form). Though currently not considered, if these provisions are deemed to extend the definition to include the instances taking place in the virtual world, the said instances can be countered. However, simply broadening the definition of these provisions will not be a long-term solution. There must be concentrated efforts to forge targeted and specific legislation that explicitly delineates and criminalizes these acts. Inspiration can be drawn from emerging global frameworks that aim to enhance user safety in online environments by imposing duties on platforms to protect users from harmful content.

V. Examining International Laws on Virtual Sexual Harassment

As global governments grapple with the novelty of VR and the fresh wave of challenges it poses, along with the dichotomy of a child's privacy and supervision against predators, sporadic attempts at regulating virtual sexual harassment are observable. The Australian Online Safety Act 2021[93] is a landmark progressive step towards developing legal mechanisms in the online space, as it actively expands digital security for Australian residents, emphasising the accountability and responsibility of online service providers and defining a clear set of expectations for them to meet. Though the Act does not explicitly curtail sexual harassment in the

[88] Bhartiya Nyaya Sanhita, s75.
[89] Bhartiya Nyaya Sanhita, s79.
[90] Information and Technology Act 2000, s72.
[91] Information and Technology Act 2000, s67.
[92] Information and Technology Act 2000, s 67A.
[93] Online Safety Act 2021 (AU).

metaverse, it does include provisions such as the requirement of online service providers and platforms to detect and remove illegal content like child sexual abuse. It establishes an Adult Cyber Abuse Scheme for those eighteen and above. The Act allows eSafety to impose industry-wide standards if online service providers cannot agree on the codes or if they develop codes that do not contain appropriate safeguards. This provision can be extended to a wider age bracket encompassing digitally active minors, and the "online service providers" can be applied to the metaverse service providers. Considering the recent decision by the Australian Parliament to ban social media for kids under the age of sixteen,[94] the question arises, 'Is banning social media altogether the right solution, or is bringing in swift legal provisions to punish those committing these crimes behind the screens and in the name of games the right way?' Along with the government, there arise the responsibilities of the intermediaries running these platforms, where a grown man and a thirteen-year-old girl can potentially communicate within rooms built for having virtual sex.

Another example is Directive 2011/92/EU of the European Parliament.[95] It highlights the severe forms of sexual abuse and sexual exploitation of children, which are increasing and spreading through the use of new technologies and the Internet. These 'new technologies' open up doors for VR, though this has not been categorically mentioned in the provision. It includes in its provisions various forms of sexual abuse and sexual exploitation of children, which are facilitated by the use of information and communication technology, such as the online solicitation of children for sexual purposes via chat rooms over the metaverse, thus providing a scope for amplification of the protection it accords. In addition, Article 36 of the Convention on the Rights of the Child[96] states that "States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare." Though it does not explicitly cast its shadow over the metaverse, with time, the article has been expanded in proportion with the digital expansion to cover online media, constantly redefining 'all.'

The Online Safety Act of the UK[97] establishes stringent provisions on online platforms against harmful content, especially that directed towards children. The regulations cover social media platforms, search engines, and other online services accessible to users in the UK. It stands apart from other legislations as it widens the scope of 'harmful content' to cyberbullying, grooming, etc., including content related to controlling or

---

[94] Hannah Ritchie, 'Australia approves social media ban on under-16s' (*BBC*, 29 November 2024) <https://www.bbc.com/news/articles/c89vjj0lxx9o> accessed 27 December 2024.
[95] Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA OJ L 335/1.
[96] Convention on the Rights of the Child, art 36 (UNGA).
[97] Online Safety Act 2023 (UK).

coercive behaviour, an occurrence prevalent in VR.[98] The goal here is not to create the same legislation but to build laws addressing the prevailing sexual harassment in VR by incorporating specific aspects from the above-discussed foreign laws. In addition, the UK Communication Act of 2003[99] could be treated as an edifice to introduce provisions for protection against indecent communication or action over public electronic communications networks and introduce punitive reparations for complicit avatars.

While newer legislations are trickling in, some previous statutory frameworks also possess the potential to be broadened to encompass the grey areas of the metaverse's security. As the metaverse involves massive data processing, companies could end up with an unprecedented wealth of physical and psychological information,[100] which can result in uniquely identifying users or providing a detailed insight into their personality, preferences, and health. The General Data Protection Regulation of the European Union[101] requires additional safeguards for data processing involving minors (under sixteen). While the GDPR applies to metaverse service providers such as Meta's data processing activities since the services are also offered in the EU, due to the unique nature of the Metaverse and the wide variety of data that will be processed, including inherently sensitive and biometric data gathered from functionalities, such as motion tracking, hand tracking, face tracking, and eye tracking, their compliance with the EU's regulatory frameworks are not straightforward.[102]

Governments and metaverse platform providers must take the unfettered presence of sexual predators and the harrowing VR accorded to minors into cognizance and prioritise policies that safeguard the interests of minors as a corollary of the advancement in immersive technology while designating accountability. The evident dearth of legislation and litigation in the same spotlight is the Achilles' heel of VR and continues to allow offenders to go unpunished for their "virtual crimes." The weight of the legal void should be acted upon, and earnest attempts at safeguarding metaverse users should be undertaken.

---

[98] 'Bangor University uses VR to give students valuable insight into coercive control' (*Prifysgol Bangor University*, 25 April 2024) <https://www.bangor.ac.uk/news/2024-04-25-bangor-university-uses-vr-to-give-students-valuable-insight-into-coercive-control> accessed 27 December 2024.

[99] UK Communication Act 2003 (UK).

[100] Brittan Heller, 'Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law' (2020) 23(1) The Vanderbilt Journal of Entertainment and Technology Law <https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1/> accessed 27 December 2024.

[101] General Data Protection Regulation of the European Union 2016 (EU).

[102] Vasilis Xynogalas and M R Leiser (Mark), 'The Metaverse: searching for compliance with the General Data Protection Regulation' (2024) 14(2) International Data Privacy Law <https://academic.oup.com/idpl/article/14/2/89/7642047> accessed 27 December 2024.

VI. Can the boundaries of real-world law stretch to regulate VR?

The world is competing in a race to position itself as a champion of immersive technology, riding on the coattails of augmented and virtual reality. Meta CEO Mark Zuckerberg has said virtual- and augmented-reality-powered devices will eventually replace mobile phones and some in-person communication.[103] With a semblance to the restructuring of the digital landscape with commercialization and integration of generative AI in day-to-day life, immersive technology will have a greater role to play in the coming decade. As pre-emptive measures, various governments and corporations are introducing policies and deals. The United States of America even introduced the United States Leadership in Immersive Technology Act[104] to cement its ambitions.[105] Following Apple's launch of its new AR headset, Apple Vision Pro, in February 2024, several companies have begun leveraging the technology to give consumers a more immersive product experience. Moreover, Disney acquired a one billion, five hundred million stake in Epic Games and announced a collaboration between the two companies to build a new virtual entertainment universe. Thus, a rapid shift towards commercially adopting VR is observable.

The undeniable fact is that VR mimics reality. Thus, the possibility of real-world crimes seeping into VR exists. However, there is no significant legislation regulating the metaverse. While modifying an order of a Sessions Court, which held a thirty-nine-year-old man guilty of groping a twelve-year-old girl and removing her salwar,[106] the proclamation of a single judge bench of Bombay HC reasoned that, as no specific detail was raised regarding the removal of the top or whether the man inserted his hand inside the top and pressed the breast of the child aged twelve years, it would not fall within the definition of 'sexual assault.'[107] While the Hon'ble Supreme Court later overturned the judgment, it raises serious concerns concerning sexual assault committed for its definition remains conflicted in the real world. Thus, contemplation arises whether sexual assault within VR would even be considered a crime or not. The Supreme Court bench reversing the order above has held that *"The most important*

---

[103] 'Mark Zuckerberg just laid out his vision for the metaverse. These are the five things you should know' *The Washington Post* (28 October 2021) <https://www.washingtonpost.com/technology/2021/10/28/facebook-meta-metaverse-explained/> accessed 28 December 2024.

[104] The United States Leadership in Immersive Technology Act 2024 (US).

[105] 'New Legislation Could Help Position US as Global Leader in Immersive Technology, Says ITIF' (*Information Technology and Innovation Foundation*, 11 December 2024) <https://itif.org/publications/2024/12/11/new-legislation-could-help-position-us-as-global-leader-in-immersive-technology-says-itif/> accessed 28 December 2024.

[106] *Satish Ragde v State of Maharashtra* (2021) SCC Online Bom 72.

[107] Sharmeen Hakim, 'Pressing Breasts Without Disrobing Not "Sexual Assault" As Per POCSO Act But Offence Under Sec 354 IPC: Bombay High Court' (*Live Law*, 24 January 2021) <https://www.livelaw.in/top-stories/pressing-breasts-without-disrobing-not-sexual-assault-pocso-bombay-high-court-168845?fromIpLogin=88023.86425039943> accessed 28 December 2024.

ingredient for constituting the offence of sexual assault under Section 7 of the Act is the "sexual intent" and not the "skin to skin" contact with the child."[108] If applied to the instance of the sixteen-year-old girl being assaulted in VR, the person who is committing the act of harassment could be held liable for the act of sexual harassment under the POCSO Act of 2012 if the presence of "sexual intent" in the psyche of such an individual is established.

Moreover, Chapter III of the POCSO Act 2012[109] addresses the issue of the use of a child in any form of media, including “any electronic form,” for sexual gratification. This provision includes the possibility of convicting a sexual offender who commits the crime of child pornography in the realm of the metaverse, provided that the term “any electronic form” covers the metaverse within its definition. It indicates that there is an increase in the prospect of the boundaries of Indian legal provisions being stretched to include sexual crimes taking place within a virtual environment. Furthermore, the proposed Digital India Act 2023[110] aims to tackle the stagnation of the Information Technology Act of 2000[111] by putting forth provisions proportionate to advancements in the digital landscape. It emphasizes women's and children's safety while acknowledging the harm the internet, devices, and information technology pose to users. As its objectives address emerging technologies, it presents an opportunity to regulate harassment in the metaverse. By employing pre-emptive measures and robust legislation, instances of such harassment can be dealt with judiciously while actively discouraging the same, allowing the users, including minors, to feel secure.

VII. From Gaps to Guidelines: Expanding Legal Protections in VR

The existing provisions tackle the challenges accrued by conventional forms of media but are ill-equipped to deal with immersive technology and the metaverse. The provisions for the same are vague and weak, leaving the netizens and metaverse users vulnerable to harassment. It presents a serious global challenge and a golden opportunity for India to step up and pioneer law-making in this field with calculative brainstorming and redefining definitions and provisions. Specific Indian legal provisions that have been discussed earlier have the potential to improve the scope of punishing predators committing sexual assault or violence within the virtual world. Starting with Section 66E (punishment for violation of privacy) of the IT Act 2000, it can be extended to punish the predators in

[108] Sneha Rao, ‘Restricting 'Touch' Or 'Physical Contact' Only To 'Skin To Skin' Contact Absurd: Supreme Court Reverses Bombay HC's POCSO Judgment’ (*Live Law*, 18 November 2021) <https://www.livelaw.in/top-stories/pocso-skin-to-skin-judgment-supreme-court-bombay-high-court-attorney-general-185784?fromIpLogin=25387.788661518385> accessed 28 December 2024.
[109] Protection of Children from Sexual Offences Act 2012, ch 3.
[110] Digital India Act 2023.
[111] Information Technology Act 2000.

some instances of harassment (such as – violating the privacy of other avatars by videotaping them, circulating images of the private parts of different avatars, etc.) in the VR, considering the definition of online platforms can further be extended to address instances of online sexual violence taking place in the metaverse.

Furthermore, Section 78 (stalking) of the BNS[112] describes the act and punishment for stalking in the real world and through electronic communication. Suppose the definition is considered for future revaluations. In that case, there is a scope to include the cases of stalking in the virtual world (something that is prevalent in the metaverse and often results in instances of simulated groping and ejaculating onto the victim's avatar) within the ambit of "electronic communication."[113] In *Animesh Boxi v State of West Bengal,* the court held that apart from online stalking, the victim suffered from "virtual rape" every time a user of an openly accessible global website witnessed the video that was uploaded by the accused. The court quoted the saying of Justice Stephen Breyer of the US Supreme Court, "In this age of science, science should expect to find a warm welcome, perhaps a permanent home, in our courtrooms… Our decisions should reflect a proper scientific and technical understanding so that the law can respond to the needs of the public."[114] The current framework is set in a way that indirectly provides a haven for sexual predators to do acts that impose a grave psychological impact upon people and minors.[115]

While revising the existing definitions and laws and bringing in new legal provisions, the accountability that the platform providers hold, along with giving away a space to experience VR reality, such as Roblox and Horizon Worlds, must not be forgotten. Taking an example of the "personal boundary" feature introduced by Meta reflects the good side of these platforms.[116] Using this safety feature, one can set up their boundary using virtual walls to prevent avatars from coming too close and limit unwelcome interactions. Roblox's recent announcement on blocking

---

[112] Bhartiya Nyaya Sanhita, s78.

[113] Kellen Browning, 'More Resignations, but No Sign Yet of a Change in Gaming Culture' *The New York Times* (19 July 2020) <https://www.nytimes.com/2020/07/19/technology/gaming-harassment.html> accessed 30 December 2024.

[114] Harsh Agrawal & Rashi Jain, 'Expounding the Contours of Sexual Harassment in Virtual Reality: Applicability of the Penal Laws to State-of-the-Art Technology (Part 2)' (*The RMLNLU Law Review Blog*, 24 May 2022) <https://rmlnlulawreview.com/2022/05/24/metaverse-2/> accessed 30 December 2024.

[115] Sheera Frenkel and Kellen Browning, 'The Metaverse's Dark Side: Here Come Harassment and Assaults' *The New York Times* (30 December 2021) <https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html> accessed 30 December 2024.

[116] Vivek Sharma, 'Introducing a Personal Boundary for Horizon Worlds and Venues' (*Meta*, 4 February 2022) <https://about.fb.com/news/2022/02/personal-boundary-horizon/> accessed 30 December 2024.

children under thirteen from messaging others on the online gaming platform is a progressive step toward safeguarding them.[117] Though the children would still be exposed to viewing public conversations by everyone, they cannot have private conversations without parental approval. It is not productive as the children can still talk to their friends. Still, it rings a bell about the problem prevalent in the chat rooms, highlighting the need for better provisions and legal mechanisms to address it. Hence, collective legal and private mechanisms by the platform providers seem to be the way to address the prevailing issue and protect minors as well as adults from the sexual violence present in VR.

VIII. Conclusion

The first-ever registered case in the United Kingdom for the virtual gang rape of a sixteen-year-old girl serves as a wake-up call to usher regulations in virtual spaces like the Metaverse and structure a mechanism that holds the perpetrators and Metaverse platform providers accountable. Moreover, in an ever-changing digital world, the lines that define virtual interaction with real-life experiences are losing their lucidity in distinction. The metaverse has emerged as a burgeoning realm of the digital world, which opens up the possibility of more virtual crimes. This points to a heightened need to protect users, especially minors, from any harassment they may face as a VR user. It is to be noted that sexual harassment, even if virtual, does inflict psychological trauma mirroring that of real-world harassment and negatively impacts the victim.

Additionally, this indicates a gap in legislation and directives. The emotional toll on victims and rising instances of virtual crimes necessitate immediate attention. There are laws in India that primarily come into play when incidents of online sexual harassment occur, such as the IT Act of 2000; however, its ambit remains narrow and does not extend to the metaverse. With global leaders in technology, such as Apple and Meta, offering VR services, increased access to VR technology is observable, and there is potential for a considerably more extensive market. There is an urgent need to establish adequate legal mechanisms addressing virtual sexual harassment.

Moreover, recent international frameworks, such as those of Australia and the United Kingdom, have initiated an attempt to regulate emerging technologies, but they are still at a point of nascence and do not explicitly include the metaverse. The existing frameworks, such as the GDPR, also require refreshing to adapt to the newer challenges of the metaverse. To effectively combat the same, it is necessary to develop comprehensive

[117] Liv McMahon, 'Roblox to ban young children from messaging others' (*BBC*, 18 November 2024) <https://www.bbc.com/news/articles/c9wrqg4vd2qo> accessed 30 December 2024.

legislation that categorically addresses virtual harassment. There is a need for defined guidelines for metaverse platform providers to hold them accountable and better safeguard the users' interests.

In conclusion, by novel legislation and expansive interpretation of existing laws and precedents, a regulatory framework can be shaped as a response to the evolving landscape of the metaverse, addressing the critical impact virtual harassment has on VR users, especially minors, fostering an inclusive and safe environment for all.

The NFT Paradox: Ownership Without Rights? A Maze of Overlapping Claims

- **Nishtha Agarwal***

Abstract

With the rise of Non-Fungible Tokens (NFTs) the digital asset ownership was revolutionized, offering new opportunities to for artists, collectors, and investors. This paper examines the impact created on intellectual property (IP) rights by NFTs and legal complexities surrounding the same. While NFTs offer a unique form of digital asset ownership through blockchain technology, they often create confusion regarding the rights actually transferred to buyers. The distinction between token ownership and copyright ownership remains blurred, resulting in challenges related to moral and economic rights, unauthorized reproductions, and the resale of digital works. Through case studies and legal precedents, the research highlights the growing conflict between creators and NFT owners, exploring instances of copyright infringement, personality rights violations, and platform liability. Additionally, the paper proposes the implementation of stronger regulations, transparent smart contracts, and mechanisms like Droit de Suite to ensure fair compensation for creators. Emphasizing the need for a balanced legal framework, this study calls for a reassessment of IP laws to address the evolving landscape of digital ownership in the NFT marketplace.

I. Introduction

As Artificial intelligence and developing technologies integrate into our daily lives, they disrupt the traditional legal frameworks. The emergence of Non-Fungible Tokens (NFTs) and blockchain technology represent one of the most significant innovations, allowing the tokenisation of digital assets on blockchain platform. It has reshaped the digital economy, opening new avenues for trading assets. However, the commercialisation of these digital tokens introduced legal challenges, particularly surrounding copyright, moral rights and personality rights of the creators.

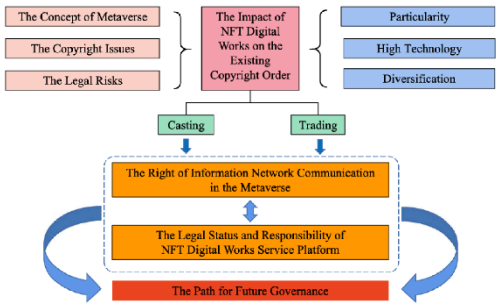
As technology advanced, the legal and ethical challenges, surrounding IP rights, also multiplied. In this context, it became necessary to differentiate between the ownership of an NFT and the IP rights associated with the underlying work. The excitement around NFTs often overshadows the fact that owing an NFT does not confer ownership of the underlying intellectual property, causing widespread confusion. Moreover, the lack of clear regulations in this area pertaining to copyright and resale rights of the NFT has allowed infringement of the creators' rights without consequence. More often than not, the buyers believe that they own more

* B.A. LL.B. (Hons.) Student at Jindal Global Law School, Sonipat

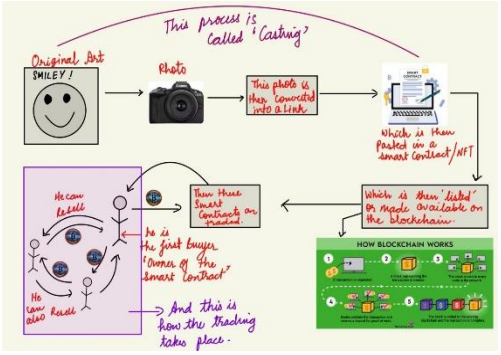
they actually have legally acquired the rights over, leading to a series of disputes.

This research critically examines the intersection of NFTs and copyright law. It argues for the development of strong regulations to curb the exploitation of rights through NFT trade and maintain the integrity of intellectual property in the digital realm. In doing so, it provides a comprehensive analysis of how NFTs challenge traditional concepts of ownership and copyright and why a re-evaluation is required for creating dynamic IP laws to adapt to the evolving digital marketplace.

II. NFTs and Ownership



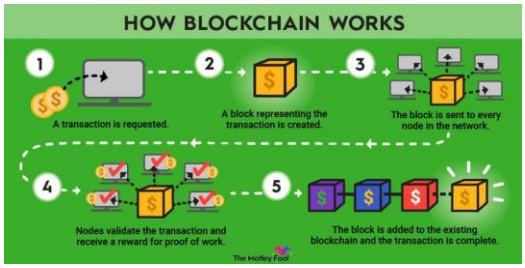
[118]An **NFT** is a unit of data stored on a blockchain, a digital ledger, deriving its value from underlying assets.[119] Unlike fungible assets like cryptocurrencies, NFTs are distinct and cannot be exchanged easily.[120] Essentially, NFTs serve as certificates of authenticity for digital or physical assets, allowing ownership to be traced and verified publicly on the blockchain while limiting unauthorized minting. The evolution of the Metaverse facilitates the entire process by allowing the seller and buyer to engage effectively, creating a high-value marketplace with numerous opportunities for all parties involved.[121]



If I take a photo of an artwork, the picture will then be converted into a link, smart contract, or a token that will be traded as an NFT, while the original artwork will remain where it is. Hence, an NFT does not contain the actual asset, but rather a reference to that asset, much like a contract stating, "Person A owns a **digital file** of Asset X," Incident to the distribution of a creator's work.

---

[118] Yupeng Dong and Chunhui Wang, 'Copyright Protection on NFT Digital Works in the Metaverse' (2023) NingboTech University, China, and Zhejiang University, China, published online 30 June 2023.
[119] Indian Copyright Act 1957, s 14 (c)(i)(A).
[120] Mark Conrad, 'Non-Fungible Tokens, Sports, and Intellectual Property Law Issues: A Case Study Applying Copyright, Trademark, and Right of Publicity Law to a Non-Traditional Ownership Vehicle' (2022) 32 J Legal Aspects Sport 132.
[121] C Wang (n 1).



[122]Under Indian copyright law, Section 17 grants the author of a work the first ownership of their creation. When read alongside Section 14(c), it becomes clear that the copyright owner has the legal right to reproduce their work in electronic form. This provision also grants them the right to issue multiple copies of their work. In essence, artists can rely on this section to create electronic copies of their work, such as NFTs, and use them for public communication, trade, and monetization. However, selling an NFT of their artwork does not equate to relinquishing their copyright. They are merely sharing their work through a different medium. The lack of awareness about this distinction contributes to the confusion surrounding NFT transactions.

Additionally, the 'principle of exhaustion' of rights does not apply to copyright in NFT digital works.[123] Unlike traditional copyright law, which allows free resale of tangible goods after the first authorized sale The *Tom Kabinet case*[124] established that online sales of e-books constitute public dissemination[125], not distribution, and are therefore outside the exhaustion doctrine. Similarly, EU law excludes NFTs from distribution rights, meaning resale or transfer of NFT-linked digital works requires the copyright holder's permission. The Hangzhou Internet Court also ruled that the exhaustion of rights doctrine does not apply to NFTs, confirming that copyright holders retain control over digital works even after the first sale. Further aggravating uncertainty regarding the rights of each party involved in the transaction.

[126]This lack of clarity leads to "Fractional Ownership," sparking the debate of ownership vs. copyright, where only the ownership of token is exchanged and not the underlying copyrights. The copyright, which includes exclusive rights to reproduce, distribute, or adapt the work, remains with the original creator unless explicitly transferred. This creates legal uncertainty, as platforms often fail to clarify the nature of the ownership. Resulting in infringements as seen in the *Ma Qianli* ***case***,

[122] Anders Bylund, 'What is Blockchain.' (The Moltey Fool, Jan 2025) < https://www.fool.com/terms/b/blockchain/>
[123] C Wang (n 1).
[124] Case C-263/18 (19 December 2019).
[125] Indian Copyright Act 1957, ss 14(ii), 14(iii).
[126] 'China copyright infringement case: China issues first court ruling on NFTS.' (Questel, June 2022) < https://www.questel.com/resourcehub/china-copyright-infringement-case-china-issues-first-court-ruling-on-nfts/>

where unauthorized NFTs were created from a copyrighted artwork, *A Fat Tiger is Getting the Vaccine.*[127]

By, virtue of the ownership of an NFT of a digital asset, there exist a rights to resell. The original owner can transfer additional rights by explicitly specifying them in the smart contract. However, the bundle of rights and T&C transmitted to at first instance may not be understood in their entirety creating hinderance when such rights are carried forward pursuant to the resale of the digital asset. As a result, a communication gap is created, which causes additional complications. This raises important legal questions about the rights an NFT dealer truly acquires.

Example:[128]

In the year 1993 Miramax, Tarantino, and his production company, Visiona, signed agreements giving Miramax rights to the film 'Pulp Fiction', including copyright and trademark. However, Tarantino reserved certain rights, including the right to publish the screenplay in various forms, such as print and electronic formats.

Later the in the year 2021 NFTs were on the rise. Eventually Tarantino launched an NFT collection featuring handwritten portions of the *Pulp Fiction* screenplay and sold them on the OpenSea platform as NFTs in the year 2021. Miramax sued, claiming that this sale violated the agreement by infringing on its copyright and trademark rights, as Tarantino's reserved "screenplay publication" rights didn't extend to NFTs. (They couldn't have foreseen the development of this technology when they first made the agreement and there was no way to include this. Also, the then present laws were not equipped enough to deal with such an issue.)

Hence this case is important as this highlights the need for developed laws plus the need to include AI based developments in future agreements. For those creating NFTs based on existing IP, it's crucial to review contracts to ensure they have the rights to do so. If NFT rights aren't clearly covered, legal disputes may arise, relying on party intent and industry norms to determine ownership and usage rights. [129]

[130]Another such example is Free Holdings vs. McCoy[131] where ownership confusion resulted in legal disputes, as it questioned whether McCoy still had rights to the first-ever NFT, Quantum. Here, Ownership of the NFT was separated from intellectual property rights. Reinforcing the importance of clarifying what rights are being transferred during NFT

[127] C Wang (n 1).
[128] Michael D. Murray, 'NFT Ownership and Copyrights' (2023) 56 Ind L Rev 367.
[129] Emily Dieli, 'Tarantino v. Miramax: The Rise of NFTs and Their Copyright Implications.'
[130]Miramax, LLC v Tarantino, 2:21-cv-08979-FMO-JC (C.D. Cal 16 November 2021), <https://www.thetmca.com/files/2021/12/miramax-v.-tarantino.pdf> accessed on 29 March 2025.
[131] 22-CV-881 (JLC).

transactions. Underscoring that NFT ownership does not automatically confer intellectual property rights.

III. The Dark Side

As discussed the buyers assume they are purchasing full ownership of the digital asset, when in reality, they may not have even obtained the right to use it. This is further exacerbated by the "Dark Patterns." Dark patterns are misleading design tactics used in websites and apps to trick users into making choices they might not have made otherwise, usually benefiting the seller at the expense of the user.[132]

As a result, they not only remain unaware of the rights associated with the NFT they just purchased but also risk buying an inauthentic asset, leaving them vulnerable to financial loss and bound by complex terms and conditions. In NFT trade Dark patterns are utilised to dupe the purchaser, taking advantage of their fragmented ownership. The complexity/length of terms and conditions of NFT sales lead users to accept them without fully understanding their implications, making them vulnerable to unforeseen legal disputes. Much like the terms and conditions of usage we agree to on daily basis of different website and applications without giving a second thought.

Editors of original artwork may also modify digital pieces to artificially inflate their value, causing buyers to overpay for works that lack authenticity. Furthermore, NFTs can be created and sold without proper authority—for instance, someone could take a photograph of artwork in a gallery, mint it as an NFT, and profit from it without the artist's knowledge, leaving buyers unaware of the original source. Similarly, individuals may use deepfake technology to create NFTs featuring famous personalities, misleading fans into believing these digital assets are officially associated with those individuals, thereby encouraging them to make uninformed purchases. And there are other such instances, For example the case of fake Pixelmon NFT which when purchased and clicked on introduces a malware in the system that would target the purchasers cryptocurrency wallets.[133] But on the flip side the rights of the original creators are also at risk.

---

[132] N Upadhyay and S Upadhyay, 'The dark side of non-fungible tokens: understanding risks in the NFT marketplace from a fraud triangle perspective.' (2025) 11 *Financ Innov* 62 <https://doi.org/10.1186/s40854-024-00684-6>

[133] Lawerance Abrams, 'Fake Pixelmon NFT site infects you with password-stealing malware." (BleepingComputer, May15, 2022) <https://www.bleepingcomputer.com/news/security/fake-pixelmon-nft-site-infects-you-with-password-stealing-malware/> accessed on 29 March 2025.

IV. Be-Wild-Ered Rights

Intellectual property rights are a set of privileges that include specific protection for the original author. Copyright is a type of IPR that stems from a creative and external manifestation of a person's imaginations, reflecting on their personality and morality. Hence, these fundament rights are retained with the original creator and are non-transferable.

Moral rights are enshrined in the Berne Convention,[134] which India is a signatory to. [135] They grant authors the right to attribution and the right to integrity. The problem of fractional ownership due the ownership v. copyright dilemma in NFT trade exacerbate and complicate the enforcement of these moral rights of the original creator. The right to sell, use and modify comes in addition to the right for ownership of anything. But when such rights lack clarity and overlap with the IP rights of the original creator the problem arises. With each alteration and resale of NFT, the moral rights of the creator are diluted.

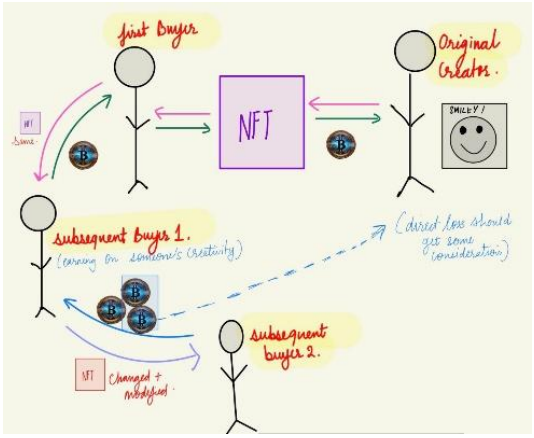
When an owner of an NFT uses the image corresponding to the code he purchased, he indirectly represents the creator/author. Given that the art has a subjective interpretation, the owner of the NFT might use the image in a way that directly contradicts the creator's ideology. Breaching the right of attribution.

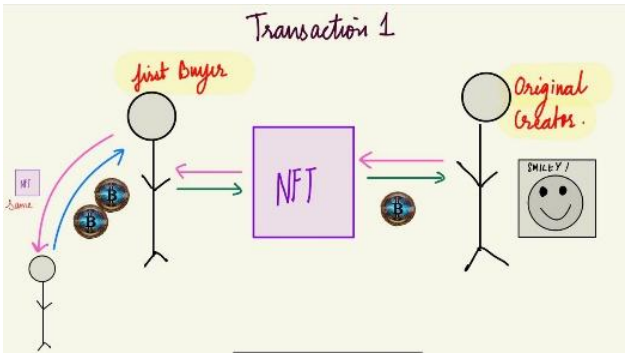
Also, when an NFT is modified, which is rather simple given that all they have to do is change the sequence of the codes, they may do so in a way that undermines the creator's integrity. Even if copyright infringement occurs, creators have limited recourse due to the ease of unchecked exchanges facilitated by technology, which complicates tracking ownership. Additionally, infringers may be unaware of the rights they are violating, further complicating litigation.

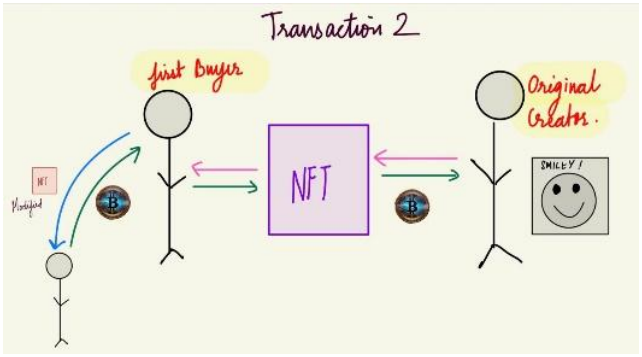
Along with the moral rights, the creator also has parallel **economic rights**. [Conflicting with the economic rights of the owner.][136] This ensures that no one can gain monetary benefits from the copyrighted artwork. The issue of resale further deepens the wound of breaches when the resale value of an NFT is greater, leaving the creator without compensation for subsequent sales.

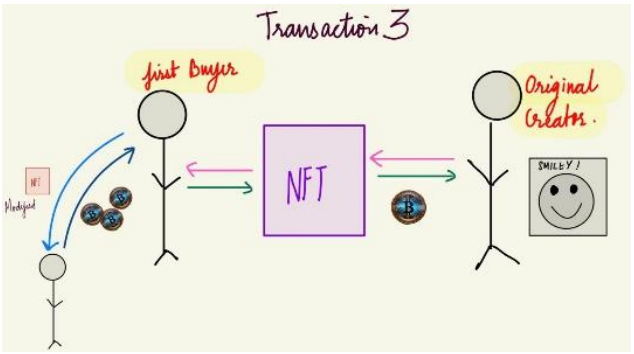
---

[134] Berne Convention for the Protection of Literary and Artistic Works, Art 6bis. (as amended on September 28, 1979).
[135] Indian Copyright Act 1957, s 57; (which allows authors to claim damages if their work is distorted or mutilated.)
[136] Gerald Dworkin, 'The Moral Right of the Author: Moral Rights and the Common Law Countries' (1994) 19 Colum-VLA JL & Arts 229.









The transactions highlight a quandary:

→ T1 – Sale at a higher price – same NFT – breach of economic rights.
→ T2 – Reselling at the same price – modified NFT – breach of moral rights.
→ T3 – Resell at a higher price – modify NFT – Breach of economic and moral rights.

T1 and T2 may not pose significant issues unless they lead to further disputes. But T3 could be problematic.

NFTs also raise concerns about **personality rights**,[137] especially when tokens represent famous individuals or public figures. Unauthorized use of likeness in NFTs can lead to identity theft. For example, Indian cases like *ICC Development v. Arvee Enterprises*,[138] where the court ruled that using a celebrity's name or likeness without permission is illegal. Similarly, when NFTs associated with a famous personality are intentionally or unintentionally[139] used in an incorrect

[137] Roberta Rosenthal Kwall, 'Preserving Personality and Reputational Interests of Constructed Personas through Moral Rights: A Blueprint for the Twenty-First Century' (2001) 2001 U Ill L Rev 151.
[138] 2003 (26) PTC 245.
[139] *Buckv Jewell-Lasalle Realty Co.*, 283 US 191, 198 (1931).

fashion it might prove detrimental to the rights of the person depicted and/or the original creator.[140]

Courts in many jurisdiction considers unauthorized reproduction, distribution, or alteration of a copyrighted work as infringement. In India this covered under Section 51 of the Copyright Act, 1957.

- → *Nike v. StockX*[141]: StockX claimed that its NFTs of Nike sneakers were simply representations of ownership of physical goods. However, Nike argued that the NFTs violated their copyright and trademarks.
- → *Hermès v. Rothschild*:[142] Artist Mason Rothschild's "MetaBirkins" NFTs infringed Hermès' IPR by creating unauthorized digital versions of their Birkin bags. Underscoring copyright and trademark violations when the underlying rights are not properly respected.

This casting and uploading without authorization is illegal and breaches many IP rights. Additionally, the resellers of a modified NFT can claim it is original art by arguing that their time, effort, skill, and creativity have gone into creating the 'derivative art,' thus asserting their own copyright. This approach can also be utilized by original creators to produce derivative works of their own creations, resulting in the evergreening[143] of copyright.[144]

For instance, the *Yuga Labs, Inc.* case highlights how derivative works of Bored Ape NFTs led to legal challenges when terms were not respected.[145] Moreover, creators often lose **economic rights** as NFTs are resold for higher values, with little to no compensation for the original artist.

---

[140] TRIPS and Berne Convention have no provision for excluding innocent infringers from liability.
[141] 22-CV-00983 (VEC)(SN).
[142] 22-cv-384 (JSR).
[143] Ifeanyi E. Okonkwo, 'NFT, Copyright and Intellectual Property Commercialization' (2021) 29 Intl J L & Info Tech 296–304.
[144]Thomas Faunce, 'The Awful Truth about Evergreening' The Age (17 August 2004) <https://www.theage.com.au/national/the-awful-truth-about-evergreening-20040807-gdyero.html> accessed 29 March 2025.
[145] BAYC Terms & Conditions, BORED APE YACHT CLUB, <https://boredapeyachtclub.com/#/terms> accessed 21 October 2024.

146

V. Confusion due to Unauthorised Reselling.

(A) Balancing of Rights

Considering these actions there is a need for an immediate reaction. There is a need for reanalysis of the existing legal framework to bring the trade of NFT under the purview of IP laws, balancing the overlapping claims of the creators and the owners of NFT. Because every action involving the display of the NFT by the purchaser can constitute an IPR infringement. Then what is the point of buying an NFT at such high price when the owner has to use his rightfully purchased property in a very restrictive manner. This dilemma demands for a refreshment of the laws so that there can be a well-defined distribution of rights amongst the purchaser, sellers and creators of NFT.

This can be achieved by utilising Smart Contracts. A smart contracts records the characteristics of the asset, the details of the issuer and other relevant details, ensuring an efficient flow of the "Digital Commodities." Essentially, when one purchases an NFT they are merely buying metadata if there no clearly defined rights attached therewith. Hence, a smart contract, fundamentally backed by encrypted codes, generates a proof of ownership of a digital asset while clearly outlining a reliable division of rights that takes place doing a transaction.

In a blockchain based smart contract one block after another in added to form a chain. Each block added is extensively verified and prevents the alteration/editing of the previous blocks. For example, 7 blocks (transactions) are added, if a anyone tries to change anything from block 3

---

[146] Samnatha Hissong, 'How Four NFT Novices Created A Billion-Dollar Ecosystem of Cartoon Apes.' Rolling stones, Nov 2021. < https://www.rollingstone.com/culture/culture-news/bayc-bored-ape-yacht-club-nft-interview-1250461/>

they will also have to make changes from block 4 to 7. Ideally, preventing any possibility of illegal alterations. Additionally, all the transactions are maintained in the form of a digital ledger. Now in the case of blockchain based smart contracts, they can design a 'fault switch' which will automatically trigger a contact between the interested parties. This reduced extra workload, third party involvement, chances of burying the fine print, blind siding, unnecessary alteration of terms etc. In this way the purchaser can get verified set of rights, so that they are not purchasing metadata just for the sake of it. For the seller/creator it ensures that no more than the rights they want to divulge is transferred. For the original creator they can make sure the description of their work is conveyed forward to the *n*-th purchaser of their work, in the form of NFT, protecting their moral and personality rights.[147]

Unfortunately, the combination of Indian laws like the Contract Act, the Evidence Act, and the IT Act allows for the recognition of smart contracts at the cost of effective recourse when disputes arise. The Indian Contract Act, 1872, establishes that a contract must include free consent (Section 14), a meeting of minds (Sections 2(a) and 2(b)), and lawful consideration (Section 10) for it to be held valid. However, smart contracts operate through self-executing code, making it difficult to establish truly informed and voluntary consent, especially since once deployed, smart contracts cannot be altered. This creates a fundamental issue with Section 14, as parties may not be able to renegotiate terms or account for unforeseen circumstances. Additionally, Section 56, which allows for a contract to be voided if performance becomes impossible (frustration of contract), is not applicable in the case of smart contracts, as they execute automatically regardless of changed circumstances. The Indian Evidence Act, 1872, does recognize digital contracts under Section 65B, which allows for electronic records as admissible evidence, and Section 67A, which mandates that electronic agreements be authenticated through digital signatures.[148] However, smart contracts do not typically use legally recognized digital signatures, making their enforceability in courts highly uncertain. Moreover, S.18 of the Indian Copyright Act states that the contract has to be in writing. Similarly, the Information Technology (IT) Act, 2000, provides for the recognition of electronic contracts under Section 10A, but it also requires digital signatures for authentication under Section 3, which smart contracts lack. This creates a major loophole—while the law allows

---

[147] Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets.' (1996) https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[148] Sharma M, Gupta S. 'E-Signing of Contracts and documents in India.' (Corporate & Commercial, 5 Aug 2021) https://singhania.in/blog/e-signing-of-contract-and-documents-in-india#:~:text=The%20Information%20Technology%20Act%2C%202000,available%20in%20electronic%20form%20and\

for smart contracts to exist, it does not provide them with the necessary legal validity required for enforcement.[149]
A potential solution could be allowing parties to a smart contract to share limited access with a government regulator, making such sharing compulsory but ensuring strict liability for the government in case of data leaks. A major benefit of implementing a government-specified blockchain registry is that it would provide smart contracts with greater evidentiary value and eliminate fraud risks, addressing one of the primary deficiencies in the current legal framework. However, blockchain-based transactions expose contract terms to third parties, potentially making them vulnerable to external litigation.
Additionally, responsibility for copyright infringement should also fall on intermediary NFT platforms, which can be held liable if they facilitate the sale, distribution, or exhibition of infringing works, regardless of claims of innocence. Courts in the US and EU have ruled that intent is irrelevant, making platforms liable as secondary infringers unless intermediary immunity applies.[150] In India, Section 79 of the IT Act, 2000 offers some protection to intermediaries that act as neutral platforms and promptly remove infringing content upon notification.[151]

However, platforms must exercise due diligence and cannot evade liability through standard terms if found negligent.

→ *Napster*:[152] held platforms accountable for user-generated infringement.
→ *Peterson v. Google LLC & Elsevier Inc.*: [153] held that platforms like YouTube are not directly responsible unless they knowingly permit copyright violations, a principle applicable to NFT platforms.

The liability of NFT platforms is a critical concern. Hence, stricter consequences for intermediaries may help correct market behaviour.

(B) Remedies at a Snapshot[154]

→ DROIT DE SUITE[155] - the right of resale, allows artists to receive a percentage of the sale price each time their artwork is resold. Ensuring that the creator benefits from the increasing value of their

[149] Apurva Agrawal, 'Block Chain and Smart Contract in India.' (July 2023) https://www.linkedin.com/pulse/blockchain-smart-contract-india-apurva-agarwal/
[150] C Wang (n 1).
[151] *MySpace Inc. v Super Cassettes Industries Ltd.*, 2016 LawSuit (Del) 6574.
[152] *A&M Records, Inc. v Napster Inc.*, 239 F.3d 1004 (9th Cir. 2001).
[153] *Peterson v Google LLC*, (22 June 2021) In Joined Cases C-682/18 and C-683/18.
[154] M Murray (n 11).
[155] Victor Ginsburg, 'The Economic consequences of Droit de Suit in the European Union,' (March 2005) European Center for Advanced Research in Economics and Statistics, Université Libre de Bruxelles and Center for Operations Research and Econometrics, Louvain-la-Neuve.

work or any share of the profit, as it is their hard work that is being traded.[156]

→ DROIT D' AUTEUR[157] – Author's Right, granting creators exclusive rights to their original works. Where they can never waive off their IP rights, instead only licence[158] their Right to Distribute.
This would be converted into the rights of the owner of the token to commercially exploit the NFT in a limited sense, such as CryptoKitties.[159] A share of which could be given to the creator in Royalties, respecting the owner's Right to Display the NFT they purchased.[160]

→ S 2 (Z):[161] Where the modifier and creator can come to terms when they share a joint right to the subsequent art produced.
If a subsequent creator invests time, effort, and creativity to modify a product, they should obtain copyright for their work, regardless of tangibility. Incidental to their right to create derivative works. The creation is fixed in the form of unique code that can be reproduced and distributed, meeting the essentials of copyright.[162]

→ A comprehensive regulatory framework: Designed to clearly define the rights of the creators, owners, purchasers, and sellers of the NFT, clearing the web of overlapping rights. Ex: make it compulsory for the creator to enlist a concise and easily visible list of rights being transferred in order to curb dark patterns.[163] For example, under the Indian Legislation, a combination of laws like the Evidence Act, IT Act, and the Contracts Act do facilitate the creation of Smart Contracts, drawing from the concept of meeting of minds, but they lack the enforcement norms, leaving a remedy seeker high and dry. Secondly, with the pace of transactions where a particular NFT keeps the ability to change multiple hands and jurisdiction within a short span of time, it is exceedingly difficult to establish privity to contract and Locus Standi.

→ Comprehensive AI law: Preventing the alteration of metadata's string of numbers that make the original NFT untraceable. Also, it is important to make sure that at the entry point, the website demands the correct set of documents, verifies the authenticity of the

---

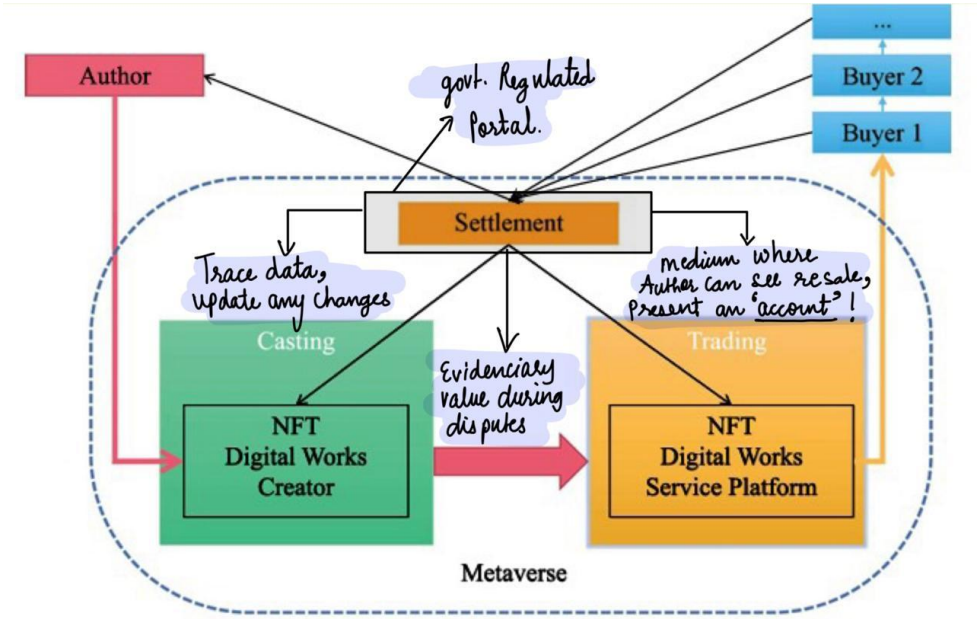
[156] *Leatherman Tool Group v Cooper Industries, Inc*. 131 F.3d 1011, 1014-15 (Fed. Cir. 1997).
[157] Rudolf Monta, 'The Concept of Copyright versus the Droit D'Auteur' (1959) 32 S Cal L Rev 177.
[158] Indian Copyright Act 1957, S 30.
[159] Terms of Use, CRYPTOKITTIEs, <https://www.cryptokitties.co/terms-of-use > accessed on 21 October 2024.
[160] M Murray (n 11).
[161] Indian Copyright Act, 1957 (14 of 1957).
[162] *Apple v. Franklin Computer Corp*., 714 F. 2d 1240 (3d Cir. 1983).
[163] Runhua Wang, Jyh-An Lee, Jingwen Liu, 'Unwinding NFTs in the shadow of IP law' (2024) 61 AmBusLawJ31.

copyright, and keeps track of changes as they come.[164] Protecting the work in the digital landscape.[165]

→ Smart contracts and blockchain technology: Enhancing transparency in NFT trade by creating a permanent public ledger of transactions, ownership changes, duration of right[166] and provenance. This transparency prevents copyright holders from obscuring rights or falsely claiming originality, as all modifications are traceable.

→ Other civil remedies like damages,[167] interim injunctions[168] on sale, fair use (as the owner has purchased it. He has paid consideration for it.)[169] and rectification of the metadata or removal of the NFT.

In this way, NFTs, if used correctly and under accurately curated laws, could offer a more transparent and equitable framework for managing the lifecycle of copyrighted works. If utilised to its full potential, such a framework of law could revolutionise copyright tracking and recording, even reducing the litigation burden on the courts to an extent.



CRAFTING A RESOLUTION/SETTLEMENT FRAMEWORK. *

[164] The EU Directives on Copyright in the Digital Single Market (2019); Digital Millenium Copyright Act 1998;
[165] WIPO Copyright Treaty 1996, art 1(4).
[166] Indian Copyright Act 1957, s 22.
[167] Indian Copyright Act 1957, s 56.
[168] Indian Copyright Act 1957, s 58.
[169] *University of Oxford and Ors v Rameshwari Photocopy Services and Ors*, MANU/DE/2497/2016; Indian Copyright Act 1957, S 52(1)(a).
**'Settlement' denotes an ideal marketplace.*

VI. Settled? No!

It is essential to protect the expression of the people in order to encourage creativity in the society. While making sure that the rights given to the copyright holder doesn't restrict the flow of knowledge. The popularity of NFTs raises questions about why people spend large sums on works available online. Maybe because the value lies in authenticity and a connection to the original creator. Example: digital images of the Mona Lisa are free online; owning an NFT signed by Leonardo da Vinci would significantly enhance its value due to its unique ownership certificate. This bragging right is tied to the original creator's confirmation, which fuels the success of NFTs.

The lack of verification processes in the NFT space, coupled with cybersecurity concerns and identity theft, undermines the trust in this authenticity. As anyone could falsely claim authorship in the absence of robust verification mechanisms. Inadvertently, NFT platforms may become venues for copyright infringement, where unverified creators exploit IP for profit. With every resale of an NFT, the rights get diluted, increasing the number of people demanding control over limited rights. Therefore, the legal landscape must adapt to protect creators and buyers alike, preventing abuse and ensuring fairness, fostering a marketplace that can create a balance between overlapping claims.

Balancing Data, Cartels and Consumerism against Anticompetitive Practices

- **Aryaman[*] and Anjali Akhariya[**]**

Abstract

Data is becoming the new oil and the assimilation of data is used for influencing choices of the consumers in any market. The study of a society can be best conducted by studying the behavior of its constituents. The tech companies collect huge amount of data from the consumers and process them with the help of algorithms. The algorithms are also used to personalize advertisements and suggestions to the consumers. The data is collected from social media, trackers installed with the apps, online activities and behaviors. The collection and sharing of data among the companies is not a new business but with the AI tools regulating most of the data, everything seems to be interconnected. Thus, forming a cartel. These cartels are at times formed by AI tools themselves when the prices at different e-commerce websites are same for a product or the sale is offered at the same time and so on. The laws regarding the cartels need to be modified for identifying the cartels formed in the digital world and the help of AI tools need to be taken for bursting the same. Also, the leniency regime regarding the cartels formed by the AI tools needs to be broader in horizon so as to include the bigger jurisdiction as AI is not limited to a geographical boundary. In this study, secondary sources such as books, research papers, news articles, blogs, case studies and legislations are referred to.

I. Introduction

American Novelist Tom Clansy says that if you can control the information then you can control the people. In the present age of emerging technologies such as metaverse becoming a reality, we are surrounded by data clouds from all sides. Artificial Intelligence is regulating the world. There have been instances of several AI-based robots that have a tendency to overtake humans in every manner.

The reliance on artificial intelligence is essential because, in the ordinary course of business, an uncountable amount of data is created every second, and it is humanly impossible to examine and manage the same. Thus, artificial intelligence is assisted. Also, the AI has the potential to monitor the details of a market in the most minute and accurate way possible.

If all the data is collected at one repository, then it creates a monopoly of data holding, and if the repositories are interconnected, then a cartel is being formed. It can be understood as the analogy of a pipeline carrying data from users' devices to a repository. With the visible effects of data

[*] Associate at Sancus Legal
[**] LLM Candidate at Rajiv Gandhi National University of Law, Patiala

carriage, it seems that the pipelines have leaks, or all the data is being deposited at a single repository, or the repositories are interconnected. However, it is affirmed that the data carriage and its modulation are powered by Artificial Intelligence.[170]

This interconnection of data collection mechanisms may lead to the establishment of a group that joins hands to control price, which is a formal or informal agreement between businesses, and they function as a single market performer.[171] This is known as cartel formation, and the participants in the cartel formation are cartel members.

The cartel members might determine the price of the commodity, market share, division of profit, etc. The cartel dominates the market and abuses its power by restricting competitors' access to relevant data, manipulating the consumer data to devise algorithms for maximum profits, and preventing others from researching the same and entering the market.[172][173] Thus, the formation of a cartel is considered an anti-competitive practice.

II. Data manipulation and AI

The natural intelligence and artificial intelligence run parallel. The human mind is a product of the surroundings and circumstances in which it resides. It observes the society and then processes information to formulate an opinion. Traders and businesspeople have mined news, information, and commentaries for decades before reaching a decision regarding investing and strategizing. In a similar manner, Artificial Intelligence works on huge chunks of data known as big data and mines it through an automated process using algorithms. Big data as a concept is defined around five aspects, which are data volume, data velocity, data variety, data veracity, and data value. The big data, after being processed and made clean and noise-free, is 'smart data'. Key attributes for data to be smart are accuracy and agility. The transformation of big data to smart data involves several folds of AI-driven processes, and once the data is processed, it connects with the customers in real time. It monitors the movement, preferences, transactions, and so on. Thus, a data library is created for every consumer. The AI processes the big data through algorithms to learn and develop, and this process is known as machine

---

[170] A Baki, K Rabie and M Ibnkahla, 'Big Data Analytics and Artificial Intelligence in Next-Generation Wireless Networks' (2017) ResearchGate https://www.researchgate.net/publication/321347258_Big_Data_Analytics_and_Artificial_Intelligence_in_Next-Generation_Wireless_Networks

[171] Shuya Hayashi and Koki Arai, 'How Competition Law Should React in the Age of Big Data and Artificial Intelligence' (2019) 64(3) The Antitrust Bulletin 447, 449–454.

[172] F Herrera, F Charte, A Rivera and MJ del Jesus, 'Big Data and Artificial Intelligence: Challenges and Opportunities' (2017) *IEEE* https://sci2s.ugr.es/sites/default/files/files/TematicWebSites/BigData/07917205.pdf

[173] Autorité de la concurrence and Bundeskartellamt, 'Competition Law and Data' (10 May 2016) http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatanal.pdf

learning. Artificial intelligence works as a functioning fluid or brain for machines. The AI is at times defined as developing machines that can think and act rationally. They no longer rely on human intervention to seek directions and process information. For example, the Global Positioning System (GPS) map services used by travelers predict the estimated time of arrival at a place, keeping the road and traffic conditions in consideration. It determines the same by processing the data that it collects while the travelers use it. It shows your moving speed, which means that it is keeping track of speed as well as the time taken to reach a spot at different times in a day. Its accuracy is determined by the average that it comes up with after processing humongous data. This study of data and its usage is making it easy for the AI tools to understand the psyche of a consumer. These AI tools influence the interaction of the consumer with the market. There is a cloud profile of every individual on the AI network, this profile contains the trajectory of online behavior of the user on various applications. It keeps a note of the financial capability and personal preferences.[174] For example, a user keeps searching for SUVs of a certain price range during the evening. The AI shall process this data and determine whether the user is inclined to buy an SUV in a certain price range. It will accordingly give personalized advertisements at the time when the user will be most susceptible to getting trapped. Further addition of data can be tracking the movement of the user, maybe they travel back from the office during the evening time, and explore purchasing a car on their mobile phone. The AI shall keep a note of the place as well as the location where the user searches for the said car or product. This is termed as behavioral microtargeting, which is one of the most successful business strategies.[175] This targeting is based on three key elements, that is, psychometric analysis conducted by collecting a huge chunk of data and evaluating the data via machine learning algorithms in order to predict the personality and character of the target person. It also predicts their weaknesses and vulnerabilities. The data is collected from various channels, for example, several studies by the University of Cambridge have shown that analysis of likes on Facebook leads to determining the personality and character of an individual. Traits such as affiliation to an ideology, sexual orientation, and pocket analysis are identifiable.[176] The likes can also predict the religious beliefs, substance consumption, and so on. In other words, it could be said that the algorithms can know more about the targeted person than their friends and family. They could even know more about the person than the person themselves. All this is possible only by monitoring online social media

[174] Panoply, 'Data Profiling Best Practices' (Panoply, 2023) https://panoply.io/analytics-stack-guide/data-profiling-best-practices/

[175] Privacy International, 'Micro-Targeting' (Privacy International, 2023) https://privacyinternational.org/learn/micro-targeting

[176] M Kosinski, D Stillwell and T Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior' (2013) 110(15) Proceedings of the National Academy of Sciences (PNAS) https://www.pnas.org/doi/full/10.1073/pnas.1218772110

behavior.[177] All the data collected is used for marketing and advertising purposes. Now, every application on a mobile phone tries to track all the activities, and the users end up disclosing all the information to avail the services.

Data analytics companies are in the business of selling personal data; they collect critical news, legal, medical, and financial information about a user and share it with technological giants that can influence our decisions about our lives. The data analytics companies are acting as cartels; they collectively have access to all the data and are exploiting it in order to gain maximum profit.[178]

III. Data collection as a business

Now, data is the new oil, and the tech giants are collecting data in the most unusual way that one can think of.[179] The users may at times respond to posts that ask them to reveal the last five emojis that they used or keep tapping the suggestions on keyboard till a sentence is formed or choosing a color out of the given options or fill out a survey form or providing an email for logging on the platforms and much more. All these are processed, analyzed, and assimilated in order to formulate an online opinion about the user and then exploit the same information to maximize profits. These are the very basic methods of direct data collection. The companies further track the users by making them agree to their voluminous licensing agreements, in which they seek all the permissions that make them legally protected. The IP addresses are tracked, and with them, complete online movement is screened. There are apps that ask for permission to continue taking screenshots of your screen and sending them to the service provider for enhancement in service. Machine learning in combination with algorithms stimulates many significant changes in the digital market. Algorithms amplify the anti-competitive problems wherein the players in a market become participants in the cartel by way of data sharing among themselves. Further, the data companies are making it a business to sell data. Most business models rely on data in the present-day digital world.[180] Data brokering markets are turning user data into a business. RELX and Thomson Reuters are two of the oldest and original data brokers. They make a product out of the data and sell it to

---

[177] David Carroll, 'How Our Likes Helped Trump Win' Vice (15 August 2017) https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win

[178] Sarah Lamdan, Data Cartels: The Companies That Control and Monopolize Our Information (Stanford UP 2022) 22–23.

[179] Tim O'Reilly, 'Data Is the New Oil of the Digital Economy' Wired Insights (23 July 2014) https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/

[180] Economic Times, 'Google Tracks Highest Private Data among Big Tech Firms: Report' The Economic Times (24 August 2022) https://economictimes.indiatimes.com/tech/technology/google-tracks-highest-private-data-among-big-tech-firms-report/articleshow/93709975.cms

government agencies and private firms.[181] This data is the main source of cartels, as all the preferences and interests of the users can be analyzed.

IV. Artificial intelligence in pricing

The impact of AI in determining market price is that the presence of AI tools in the market undermines the prisoner's dilemma, where the two competitors are unable to communicate and engage in price wars with one another. This results in consumer gain, but with AI, the opposite is observed. The prices rise uniformly, and the consumers have no other option but to purchase the goods and services at elevated prices. The algorithms provide several ways in which the competitors in the market may collude. With e-commerce, this may even become a greater challenge where all the details are open.

With the ever-increasing usage of big data and pricing algorithms to set new pricing models and predict market trends, tactic collusion is rising. Tactic collusion is a situation where a few businesses act in a particular manner without any interaction. They collude indirectly to maximize benefits, resulting in a compromise of customer welfare[182] and regulating prices.

There are several modes that are used in algorithm pricing, such as the Messenger model, the Hub and Spoke Model, the Predictable Agent, and the Digital Eye or Self Learning Algorithms.[183] Under the Messenger Model, the algorithms are just used to work upon the deliberation of humans. It is just a mode and nothing more. In the Poster Cartel Case (United States of America v. David Topkins, 2015), two companies used Artificial Intelligence-based algorithms to regulate the prices of posters on e-commerce market platforms, which was pre-agreed between the parties. The two companies were based in the US and the UK; agencies from both countries held them guilty and imposed fines.[184]

There are Monitoring Algorithms that work to monitor the actions of competitors of the respective business and enforce a collusive agreement. Under this head, the tool may collect information regarding business decisions, data screening, market behavior, and others. The data collected

---

[181] Sarah Lamdan, Data Cartels: The Companies That Control and Monopolize Our Information (Stanford UP 2022) 58.

[182] Yadav and Tarun Donadi, 'Tacit Collusion and Artificial Intelligence' (2021) 1 *Indian Journal of Artificial Intelligence and Law* 18.

[183] Ananya Deb, 'Algorithmic Collusion: Can the Competition Act Protect against Self-Learning Algorithms?' IndiaCorpLaw Blog (4 January 2022) https://indiacorplaw.in/2022/01/algorithmic-collusion-can-the-competition-act-protect-against-self-learning-algorithms.html

[184] Diane Bartz, 'E-commerce Exec Pleads Guilty in U.S. Antitrust Case' Reuters (6 April 2015) https://www.reuters.com/article/us-usa-antitrust-ecommerce-plea-idUSKBN0MX1GZ20150406

is now processed in the algorithm, and the relevant part of the automated data is forwarded to a new set of algorithms for colluding.

In the Hub and Spoke model, competitors rely on third parties to analyze the market and decide upon the prices of their respective goods and services. Once the reliance on these third parties reaches a certain point, the third parties facilitate collusion. As the name suggests, several companies (spokes) are connected to one hub, like a wheel. Cab service provider Uber, for example, acts as a hub with the drivers as spokes. Uber uses algorithms to determine the price for travel. At certain times, the prices of the drives are high. It is AI that analyzes big data with respect to travel and applies algorithms to calculate when to surge the price and when to keep it nominal. The algorithm also keeps note of the price offered by the competitors so that the customer does not shift to alternative means. This is the reason behind the surging and decreasing prices of cabs on all service providers simultaneously.

In the method of Predictable Agent, the algorithms are designed in such a manner that they tend to modify prices without any human interference. The algorithms act as predictable agents and keep modifying the prices, which is often called algorithm-enhanced continuous parallelism. An example is the pricing of the book, "The Making of a Fly". Two artificial intelligence tools strictly followed the algorithms, and due to the absence of a price cap, it reached $23,698,655.93 (23+ million dollars) plus shipping charges for one copy.[185] This error became evident because of such an exorbitant rise in the price of the book. The errors are oblivious at times because of similar pricing everywhere, and it takes place at the expense of consumer welfare. American writer Isaac Asimov had devised the Three Laws of Robotics, which were "it may not injure or cause harm to humans, obey orders given by humans except when it contravenes the first law of not injuring or harming humans. Lastly, the robot must protect its own existence as long as it does not contravene the other two laws."[186] Now the challenges are changing, and it would be precise to propose that the AI shall never try to overpower natural intelligence. The newly proposed laws could be understood as restricting the dominance of the machines, but technological development is already at a pace that the law is unable to match. If the AI pledges not to overpower natural intelligence, then it will be in the larger interest of humankind. However, an antithesis to this is that if a machine starts thinking, then it might not follow human-made laws. AI, with its capabilities, can prove to be both useful and harmful; thus, if a machine starts thinking, then it might start to search for rationality in

[185] Olivia Solon, 'How a Book about Flies Came to Be Priced $24 Million on Amazon' *Wired* (2011) https://www.wired.com/2011/04/amazon-flies-24-million/

[186] Evan Ackerman, 'Asimov's Laws Won't Stop Robots from Harming Humans, So We've Developed a Better Solution' Scientific American (19 March 2021) https://www.scientificamerican.com/article/asimovs-laws-wont-stop-robots-from-harming-humans-so-weve-developed-a-better-solution/

human-made laws. It might obey the laws that it deems fit and disobey the rest. Law and technology have inherent contradictions. While technology knows no boundaries, it is internationalized and globalized, and the law, on the other hand, is restricted to certain geographical boundaries.[187] Thus, following local laws would be a tedious task for the AI tools. The rule of law carries a notion of reciprocity between the government and the governed. Law shall be equal for all, and no one shall be above it.[188] In the case of AI tools, there are several risks, such as data privacy and sovereignty, that shall be discussed later in this research work.

Another method is the Digital-Eye Model, which embodies the ultimate level of sophistication of algorithms. It is also known as self-learning algorithms or black-box algorithms. These algorithms are achieving a God-like view of the marketplace. They have the ability to anticipate the changes in the market and plan for optimal pricing to achieve maximum profit. Since there is no human intervention in this collusion, the cartel thus formed cannot be objected to on the basis of intent to cheat or defraud the customers. It becomes very difficult for agencies to find evidence and establish that the practice was anti-competitive.[189] One example of self-learning algorithms could be search engines monitoring web searches and selecting the ads and news that are recommended. Time and place are also significant under this recommendation.[190] This intelligence is achieved by AI tools with the concept of Machine Learning. It would be apt to reiterate that algorithms are the applications that provide reasoning to Artificial Intelligence.

Artificial Intelligence, particularly Machine Learning algorithms that are used to monitor business decisions, may tacitly collude on their own. The flight prices are one such example. The prices are often at the higher end during festive times, weekends, and holidays. If 10 people search for a flight from place A to Place B, 10 times a day, the prices will rise. It is AI that monitors customer behavior. It not only keeps suggesting flights to the customer but also regulates the price as per the demand, and the customer starts getting advertisements about the place of destination, say, cab services, hotels, places to visit, and so on. Therefore, all the data repositories are interconnected, or maybe there is a single data repository.

The most common form of collusion is through signaling. If a business raises the price of goods and services with the hope that the competitors

---

[187] Tarek R Besold and others, 'AI and the Rule of Law' (2021) Artificial Intelligence and Law https://link.springer.com/article/10.1007/s10506-021-09294-4

[188] Stanford Encyclopedia of Philosophy, 'The Rule of Law' (First published 1996, rev. 2023) https://plato.stanford.edu/entries/rule-of-law/

[189] Ania Thiemann and Pedro Gonzaga, 'Big Data: Bringing Competition Policy to the Digital Era – Background Note by the Secretariat' (OECD Competition Division, 2016) https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

[190] Martin Elbers, 'Algorithms and Law' in *The Algorithmic State – EULEN Working Paper Series* (2022) 61 https://jmn-eulen.nl/wp-content/uploads/sites/575/2022/05/WP-Series-No.-24-22-Why-do-Competition-Authorities-need-Artificial-Intelligence-Lorenzoni.pdf

will do the same, and if the competitor actually does the same, then the former's raising of price is conceptualized as an offer of a unilateral contract. By raising the prices, the competitor accepts the offer. In digital markets, it is practiced by AI. The tech giants use algorithms, and these algorithms signal to the competitors. The signaling is a real-time process. On the two biggest e-commerce platforms, the discounts and deals are almost identical.

V. Companies, Cartels, and Anticompetitive Practices

The algorithms pose the greatest challenge to competition. A few tech giants control most of the Artificial World (Virtual/Technological World). The giants have hijacked the internet ecosystem and are exploiting the cross-market presence by using their massive database. The data analytics companies mix research and financial news to advise investors and predict the projects that might make the biggest profit. Algorithmic discrimination is also a challenge to tackle, where different pricings are applied for the same products. It is when the algorithms favor their own products, as happened in the Google Shopping case, or when the algorithms favor the companies that pay higher commissions by placing their goods or services in priority on the list, as compared to the competitors, as it happened in the Trivago case.[191] Trivago's business model compares the prices of hotels on different websites and offers the best deal to customers. Its revenue is based on cost-per-click payments from the online booking sites. It was found that the hotel room rates were misquoted on its platform and television ads, highlighting the hotel booking sites that willfully paid the maximum commission to Trivago. An algorithm was used by Trivago to display such high commission-paying websites on top, but it did not actually highlight the most beneficial deals for the customers. Customers were also tricked by the usage of different colors, strikethrough prices, deceptive comparisons, and so on. It led the customers to believe that it is impartial and transparent in pricing.[192]

In one of the most talked-about data scandals in the history of humankind, the Cambridge Analytica Data Scandal. Personal data belonging to millions of social media users was collected by the British consulting firm Cambridge Analytica. The Firm used the data to set the political ground. The data of around 87 million users was collected from Facebook profiles and used to influence Donald Trump's 2016 presidential campaign. It also played a vital role in interfering with the Brexit referendum. The

[191] ACCC, 'Trivago Misled Consumers about Hotel Room Rates' *ACCC Press Release* (20 January 2020) https://www.accc.gov.au/media-release/trivago-misled-consumers-about-hotel-room-rates

[192] David Ingram, 'Facebook Says Data on 87 Million Users May Have Been Shared with Cambridge Analytica' *Reuters* (5 April 2018) https://www.reuters.com/article/us-facebook-cambridge-analytica-trump-idUSKBN1GW2UV

campaigns involved psychographic profiling, which determined the personality traits of users based on their online social presence. The advertisements are categorized differently for Trump supporters and the swing voters. The CEO of Cambridge Analytica, Alexander Nix, described that the job was to identify the ones that could be enticed to vote for Trump, which was done by showing images of notable supporters of Donald Trump and presenting a negative image of the opponent.[193] In the long-fought battle, Meta, the owner of Facebook, paid $725m to settle legal action for the data breach to Cambridge Analytica.[194]

Facebook's German Cartelization Case[195] – Facebook is not just a social connection platform; it also connects users with advertisements and publications by several businesses and associations. The revenue model of Facebook depends on online personalized advertising, which is also called target advertising. The platform uses algorithms to track the online movements of users with the aim of presenting them with advertisements that are best suited to their needs and requirements. The factors that the algorithms take note of are personal commercial behavior, their interests, purchasing power, and living conditions, as described above in the Cambridge Analytica case. The data is collected from different sources and combined to reach a conclusion. This data is again big data, and again, there are algorithms that process the big data.

This came in notice of the Federal Cartel Office (FCO) of Germany, and it was further found that Facebook has dominance in the social media market, with 95% of daily and 80% of monthly social media users preferring Facebook. The FCO concluded that Facebook has abused its dominant position and forced users to share data from other Facebook services, such as Instagram, Oculus, Masquerade, and WhatsApp. The personal data of users collected over the platforms was leveraged for Facebook's personalized advertising business.[196] This information was processed and shared across the platforms and had the potential to influence the commercial behavior and purchasing habits of the users.

---

[193] Joe Tidy, 'Facebook Fined for Misleading Users about Data Use' *BBC News* (22 December 2022) https://www.bbc.com/news/technology-64075067

[194] Eryk Mistewicz, 'Social Media Platforms' Rush on Personal Data and Competition Law: Facebook Decision of German Federal Cartel Office' *Academia.edu* (2020) https://www.academia.edu/42681831/Social_Media_Platforms_Rush_on_Personal_Data_and_Competition_Law_Facebook_Decision_of_German_Federal_Cartel_Office

[195] Rishabh Bajoria, 'German Court's Antitrust Decision Rules against Data Collection by Facebook' *IndiaCorpLaw Blog* (10 June 2020) https://indiacorplaw.in/2020/06/german-courts-antitrust-decision-rules-against-data-collection-by-facebook.html

[196] *Inc42*, 'SC Lists WhatsApp Data Privacy Case for Final Hearing on January 17' (5 January 2023) https://inc42.com/buzz/sc-lists-whatsapp-data-privacy-case-for-final-hearing-on-january-17/

To its defense, Facebook took the stand that the company processes data in order to serve the users in the best possible way and maintain the interests of Facebook.

The German Court further found Facebook's conduct to be anti-competitive as it combined data generated outside of Facebook.com with the consent of the users. It was in contravention of the General Data Protection Regulation (GDPR). Also, the Court observed that Facebook is the single largest player in the social media market with no competition. The users are not left with any alternative, nor are they allowed to choose the data that can be disclosed.

In the Indian context, the widely publicized case of WhatsApp privacy policy was in the same regard. WhatsApp was bought by Facebook in 2014, and later, they introduced changes in their privacy policy that facilitated the sharing of data between WhatsApp and Facebook, including the chats.[197] The policy was violative of the Right to Privacy under Article 21 of the Indian Constitution. In 2023, the Supreme Court of India directed the social media service provider to give a wide public undertaking that it shall not limit the functionality of the application for users who do not agree to the new privacy policy until the Indian government introduces a data protection law.[198]

Zomato's Case – The user's experience, feeling the craving for food, and then getting suggestions from the food delivery applications. Maybe the users have spoken to someone in the vicinity about having Italian food, and then the app suggests Italian cuisine with special discounts. The users are under continuous surveillance.[199]. The online dependency on these platforms has exacerbated the concern of data security, and the intersection of data, imbalances of information, and intelligent marketing has opened up new opportunities for the algorithm-based businesses to exploit the biases of the users.

The companies might have a food pattern of every individual with categories such as days of the month on which orders are placed, the time at which the person feels the urge to eat something, and at the beginning of the month, people tend to spend more.

There are features such as only two rooms at a certain price, 10 people looking for rooms right now, or 10 people looking at the XYZ flight right now. The AI is trying to influence the decisions in real time. With such features, the platforms play with the psychology of the users/customers.

---

[197] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

[198] *The Indian Express*, 'Supreme Court Asks WhatsApp to Publicise Undertaking to Government' (2 April 2023) https://indianexpress.com/article/india/supreme-court-whatapp-privacy-policy-data-protection-law-8418829/

[199] *The Star*, 'Pandemic Surveillance: Is Tracing Tech Here to Stay?' (11 March 2022) https://www.thestar.com.my/tech/tech-news/2022/03/11/pandemic-surveillance-is-tracing-tech-here-to-stay

They exploit the feeling of insecurity and scarcity of services or products. It enhances the validity in the psyche of the user that the place is worth looking at, as many others are also considering staying there and like things. This gets legal protection with the cocktail of hassle-free agreement to Terms and conditions, privacy policies, and widespread lack of understanding regarding behavior in the online atmosphere. All the information is put through algorithms to determine the ad suggestions, as it is humanly impossible to keep an eye on every movement of every user.

In yet another case, Google was accused of abusing its dominant market position by mandating registration on its platform to get a license to the Android operating system for smart devices, the Play Store, and other features.[200] The Competition Commission of India (CCI) imposed a fine of Rs. 1337.76 crores on Google for the abuse of its position.[201] In addition to the monetary penalty, the antitrust watchdog, CCI, issued several directions to Google, like not denying access to Play Services plugins to disadvantaged Original Equipment Manufacturers and not mandating the installation of Google Search, Chrome browser, Gmail, and other applications as a prerequisite. The CCI further observed that the competitors of Google could not attain the pari passu market hold as Google because of its Mobile Application Distribution System (MADA), network barriers, and certain other factors. Thus, the stated imposition of penalty was imposed for violating Section 4 of the Competition Act, 2002.[202]

VI. Legal Standpoint

A cartel is like a secretive group that may not have any absolute trace. The Competition Act of 2002 makes participation in a cartel formation an offence, within the meaning of Section 3(3)[203]. The formation of a cartel usually gives rise to abuse of dominant position that is defined in Section 4 of the Competition Act. Usual acts of abuse of dominance involve certain listed activities. They are direct or indirect control exercised by imposing discriminatory pricings, hiked pricings, predatory pricings[204], limiting or restricting the supply of goods and services, denying market access, using

---

[200] *The Indian Express*, 'Explained: Why Google Was Fined by the Competition Commission of India' (21 October 2022) https://indianexpress.com/article/explained/explained-economics/google-android-devices-competition-commission-india-fine-explained-8222377/

[201] *Business Standard*, 'NCLAT Directs Google to Pay 10% of Rs 1,337 Crore Penalty Imposed by CCI' (4 January 2023) https://www.business-standard.com/article/companies/nclat-directs-google-to-pay-10-of-rs-1-337-crore-penalty-imposed-by-cci-123010400362_1.html

[202] Press Information Bureau, 'Government of India Press Release' (27 October 2022) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1869748

[203] *The Competition Act 2002*, No. 12 of 2003, Acts of Parliament, Government of India.

[204] T Ramappa, *Competition Law in India* (2nd edn, Oxford University Press 2010).

power to influence the other party into entering a contract. Reducing the supply quantity is also an abuse of dominance, as it results in an increase in price. The demand-supply principle is applicable.

Further, Section 27(b) provides the clause for punishment in case of cartel formation. The punishment shall carry imposition of a penalty equal to thrice the profit made out of transacting with the cartel or 10 percent of the average turnover of the cartel of the preceding three financial years, whichever is higher. The act talks about Appreciable Adverse Effect on Competition (AAEC), which includes activities that restrict competition in a market, and the formation of Cartels is covered under AAEC. In plain words, the cartels are groups of businesses that come together, explicitly or implicitly, and regulate the market as per their whims and fancies; they fix prices, limit the supply of goods or services in order to make maximum profits.[205] The thirty-second report on Competition Policy 2002 by the European Union says that Cartels diminish social welfare and do the opposite, i.e., transfer wealth from consumers to parties in the cartels by modifying the output or price in relation to market-driven levels.[206]

As mentioned several times, identifying a cartel is one of the most tedious tasks; the Indian legal system has diluted the rigidity in terms of the standard of proof to be relied upon for establishing a cartel. In re Sugar Mills[207], the CCI demanded evidence that alleged participants in the cartel met and decided upon the collusive conduct. They demanded conclusive evidence of the meeting of minds. However, later in the LPG cartel case, the CCI held that cartel formation is not a criminal offence, and the test of proof shall include a balance of probabilities[208] and the liaison of intention test. [209][210] Again, in Builders Association of India v. Cement Manufacturers Association[211] also known as Cement Cartel case, the CCI held that mere presence of circumstantial evidence in the absence of any direct evidence can be conclusive.

---

[205] European Commission, *Competition Policy Annual Report 2002* (European Commission 2002) https://ec.europa.eu/competition/publications/annual_report/2002/en.pdf

[206] *In Re: MCX Stock Exchange Ltd and Others*, Case No. 1 of 2010, Competition Commission of India.

[207] *In Re: Aluminium Phosphide Tablet Manufacturers*, 2012 SCC OnLine CCI 11.

[208] Cambridge Dictionary, 'Balance of Probabilities' (Cambridge University Press) https://dictionary.cambridge.org/dictionary/english/balance-of-probabilities

[209] SCC Online Blog, 'Cartelisation: Understanding the Concept under Indian Competition Law' (SCC Online, 15 February 2021) https://www.scconline.com/blog/post/2021/02/15/cartelisation/

[210] In Re: Alleged Cartelisation in respect of zinc-carbon dry cell batteries market in India, 2012 SCC OnLine CCI 42.

[211] Nishith Desai Associates, 'The Curious Case of Leniency under the Competition Act, 2002 in India' Mondaq (21 February 2019) https://www.mondaq.com/india/cartels-monopolies/816022/the-curious-case-of-leniency-under-the-competition-act-2002-in-india

The Competition Commission of India provides for an option of leniency where any member of the cartel can honestly disclose the existence of the cartel and help the authorities in busting it. Section 46 of the Competition Act provides for such provision. The whistleblower in this case can be granted complete exemption from penalty. The Commission introduced the Competition Commission of India (Lesser Penalty) Regulations, 2009, in pursuance of Section 64 of the Act to strengthen the leniency regime. In the case of zinc-carbon batteries, the Commission granted a 100% leniency to the applicant as it disclosed the anti-competitive conduct when the Commission had no prima facie opinion about the same.[212]

The formation of cartels leads to a loss of competitiveness and thus impacts the employability factor of a society. In the case of AI-forming cartels, the view will be different from that of a traditional market. Big data, algorithms, artificial intelligence, privacy concerns, and several other factors are involved in technological cartels, which will be discussed in subsequent sections. The biggest challenge includes furnishing proof against the constitution and operation of cartels.

VII. Challenges and Suggestions

The technological development is taking place at a very fast pace, and legal development is unable to keep pace. The reason behind this is that the procedure to establish any law is too time-consuming, while the development of technology can take place in a relatively shorter time. The data-driven mergers of tech giants like Microsoft-LinkedIn, Facebook-WhatsApp, and others are posing an even greater challenge to law agencies to protect the users from being exploited, as it is getting tougher to identify and bust a cartel. These algorithms are not comprehensible to the general public. The biggest challenges might include the authorities' inability to determine the algorithms and their codes. Identifying the codes of the algorithms might help the agencies in building a counter to fight the cartel formation. This fighting technology with technology would require reverse engineering to rescue the AI cartels from bursting. Furthermore, the laws can be made more stringent in terms of revealing and collecting data.

Another challenge with artificial intelligence is the application of laws. There can be a situation where AI disagrees with human-made laws. It might make laws and rules of its own, and might as well force humans to follow the laws that are made by the AI. The German and French authorities are conducting a joint study to analyze the challenges relating to algorithms and competition law. The European Commission

[212] Soumyarendra Barik, 'Big Tech Will Have to Open Up Their "Black Box" Algorithms for Regulatory Scrutiny: EU Competition Head' MediaNama (26 November 2020) https://www.medianama.com/2020/11/223-digital-services-act-algorithms/

introduced the Digital Services Act, which focuses on collecting information and getting the analysis done of the algorithms that are used by data analytics companies and their impacts on the market and competition law.[213] The United States recently introduced the Algorithmic Accountability Act of 2022, which mandates data possessors to assess the impacts of the automated algorithmic systems that they use and sell. It further seeks to detail when and how the automated systems are used and empowers customers to make informed choices about decisions that are based on algorithmic calculations.

Thus, it can be concluded on the note that the technological development shall be made to an extent where they do not overpower humans. The identification of cartels formed by AI tools shall be monitored, and assistance from AI tools can be taken. The leniency regime regarding the cartels formed by AI tools needs to be introduced, and the tools need to be trained in such a manner as to promote competition in the market. Data collection and usage shall be properly regulated, and the new data protection bill is a silver lining in protecting the data. The right to be forgotten shall be made an intrinsic right under the Right to Privacy. Above all, the AI tools shall be trained in such a manner that they do not indulge in anti-competitive activities, and the dependency on them shall be duly curtailed so as to maintain a balance between data and its usage against consumerism.

[213] *Competition Commission of India v Coordination Committee of Artists and Technicians of W.B. Film and Television and Ors* (2017) 5 SCC 17.

AI Liability: Solving the Attribution Problem in Autonomous Systems

- **Atheestha MV***

Abstract

This article explores the emerging legal regimes that grapple with liability attribution in autonomous artificial intelligence systems. As AI technologies continue to function with limited human intervention, conventional liability models premised on human agency are severely challenged. Based on an examination of nascent case law and regulatory solutions across jurisdictions, this article advances a hybrid liability model that strikes a balance between innovation incentives and consumer protection. The model suggests elements of developers' strict liability but with an awareness of users accessing intricate AI systems. It satisfies the existing liability gap within prevailing jurisprudence while achieving a higher level of legal certainty within a sector involving accelerating technological innovation.

I. Introduction

The exponential spread of autonomous AI systems across the domains of medicine to transport has thrown open unforeseen legal complexities related to attributing liability[214]. Identifying the culpable entity—creator, launcher, operator, or the AI machine itself—whenever harm results from an AI system raises an intricate legal challenge for classical frameworks of torts to tackle[215]. The following article surveys some novel concepts toward AI liability by courts in jurisdictions around the globe and recommends an equilibristic model working for innovation and accountability concerns in harmony.

This legal challenge is made more complicated by the technological sophistication of contemporary AI systems, and especially those involving deep learning architectures that develop over time through exposure to data rather than programming[216]. These kinds of systems might adopt behaviors and decision-making patterns that their designers do not foresee or completely grasp, leading to a "rise" that makes classic notions at the center of negligence law more complicated. Courts are more frequently confronted with cases where strict product liability or negligence structures fail to fully capture the distributed nature of AI

* LLM student at Sree Narayana Law College.

[214] Mark Lemley and Bryan Casey, 'Remedies for Robots' (2019) 86 University of Chicago Law Review 1311, 1315-18.

[215] Matthew Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2016) 29 Harvard Journal of Law & Technology 353, 362.

[216] Gary Marcus, 'Deep Learning: A Critical Appraisal' (2018) arXiv:1801.00631, accessed 10 April 2025.

development and function[217]. The global aspect of AI liability adds another layer of complexity because such systems tend to be spread across jurisdictions with uneven regulatory schemes. While the European Union has progressed toward a holistic regulatory framework with the AI Act, the United States has continued generally with a sector-specific approach, generating legal contradictions that raise uncertainty for consumers pursuing remedies and companies building AI technologies[218]. Fragmented legalities have the risk of generating innovation "safe havens" with suboptimal liability standards, undermining international attempts to promote responsible AI development and generating competitive liabilities for companies with operations in better-regulated markets.

II. The Attribution Problem

Traditional liability frameworks rely on the aforementioned principles of human agency and predictability[219]. Yet, autonomous AI systems tend to run by opaque decision-making processes that are not known or easily predictable to their developers[220]. It leads to the "black box" issue, which is a serious blow to the negligence model-based current liability. When an AI-based medical diagnosis program diagnoses a malignant tumour or an autonomous car makes a fatal choice, assigning blame is legally questionable[221].

The fundamental question is: How can legal systems fairly allocate liability when decisions are increasingly delegated to systems with functions that surpass human understanding? The various parties involved in AI systems, such as the developers, data sources, users, and institutions using the technology, complicate this further[222].

What legal analysts have termed the "many hands problem"—the widespread nature of AI development and deployment, with numerous actors playing a role in the end product—compounds this attribution problem[223]. Machine learning models typically include pre-trained modules, third-party data sets, and open-source libraries, creating a web

---

[217] Ryan Abbott, 'The Reasonable Computer: Disrupting the Paradigm of Tort Liability' (2018) 86 George Washington Law Review 1, 15-19.
[218] Mark Findlay, 'Principled Regulation of AI: Beyond a Human Rights-Based Approach' (2024) 14 International Data Privacy Law 32, 45-47.
[219] Anthony Casey and Anthony Niblett, 'Self-Driving Contracts' (2017) 43 Journal of Corporation Law 1, 13-15.
[220] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015) 8.
[221] Ryan Calo, 'Robotics and the Lessons of Cyberlaw' (2015) 103 California Law Review 513, 532-535.
[222] Jack Balkin, 'The Three Laws of Robotics in the Age of Big Data' (2017) 78 Ohio State Law Journal 1217, 1223-1225.
[223] Helen Nissenbaum, 'Accountability in a Computerized Society' (1996) 2 Science and Engineering Ethics 25, 29-32.

of possible liability that resists traditional concepts of proximate cause. When injury results, it becomes almost impossible to distinguish the negligent contributor within available legal structures seeking distinct causal links as opposed to probabilistic causations[224].

III. New Methods

1. Strict liability of developers

Several jurisdictions have begun to experiment with forms of strict liability for AI developers[225]. The European Union's AI law proposes a risk-based approach, with developers of "high-risk AI systems" facing higher liability standards[226]. This approach treats AI systems as products, placing primary responsibility on those who create and market them.

The benefit of this method is that it is clear and provides incentives for full testing and security measures. Critics point out, though, that excessively burdensome liability standards can suppress innovation and confer disproportionate regulatory advantages to large corporations who are better positioned to absorb the costs of liability[227].

Supporters of strict liability point out that developers possess the highest technical knowledge of their systems and have a special ability to identify and prevent potential harms at the design phase[228]. This solution draws conceptual analogies with strict liability provisions for ultra-hazardous activities, acknowledging that certain AI applications involve inherent risks that cannot be entirely avoided by reasonable care. The UK House of Lords AI Committee has argued that when AI systems act independently in sensitive areas, strict liability can be imposed on the basis of asymmetry of knowledge between creators and those injured[229].

Implementation of strict liability frameworks also differs substantially from one jurisdiction to another. Proposed amendments by Germany to its product liability act would treat software, including AI systems, as "products" irrespective of whether they have tangible or intangible forms,

---

[224] Maayan Perel and Niva Elkin-Koren, 'Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement' (2017) 69 Florida Law Review 181, 201-205.
[225] European Commission, 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust' COM(2020) 65 final, 12-15.
[226] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence' COM(2021) 206 final, 27-31
[227] Margot Kaminski, 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2019) 92 Southern California Law Review 1529, 1574-1576.
[228] Mireille Hildebrandt, 'Smart Technologies and the End(s) of Law' (Edward Elgar 2015) 174-178.
[229] House of Lords Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?' (HL Paper 100, 2018) para 317-323.

hence covering strict liability to purely digital systems[230]. In contrast to Singapore, Singapore has taken a more conservative stance in its Model AI Governance Framework with voluntary use of liability steps and refraining from mandatory liability provisions that can be detrimental to innovation in its burgeoning technology market[231].

2. Control theory approach

Another framework that is centred on control of operations as opposed to development. In this framework, liability falls on those who deploy and run AI systems, which would relieve developers of blame once the systems are in place in given contexts[232]. This framework is aligned with classical principles of high-level responsiveness, where employers are responsible for employee conduct. A control theory solution that efficiently controls the deployment context can induce perverse incentives for developers to cut security investments while passing risk down[233].

The control theory solution has been especially prominent in medical AI environments, where medical professionals use professional judgment in conjunction with algorithmic suggestions. Courts across some jurisdictions have now started imagining the relationship between physicians and AI-based diagnostic programs to be equivalent to consultation with other experts, leaving the treating doctor with ultimate control over the integration of algorithmic recommendations into clinical judgment[234]. The approach honours the contextual situation in implementing AI while maintaining conventional frameworks of liability in professional negligence.

A significant limitation of the control theory is when dealing with completely autonomous systems that function with little human intervention. As systems achieve greater autonomy, the concept of "meaningful human control" becomes increasingly difficult, creating an accountability gap where developers or operators do not exercise sufficient control to justify the attachment of liability. This limitation has prompted regulatory initiatives such as the EU's proposed mandatory human oversight requirements for high-risk AI applications, which effectively

---

[230] German Federal Ministry of Justice, 'Draft Amendment to the Product Liability Act' (Referentenentwurf, February 2023) Section 2(1).

[231] Personal Data Protection Commission Singapore, 'Model Artificial Intelligence Governance Framework' (2nd edn, 2020) 27-31.

[232] A. Michael Froomkin and others, 'When AIs Outperform Doctors: Confronting the Challenges of a Tort-Induced Over-Reliance on Machine Learning' (2019) 61 Arizona Law Review 33, 61-63.

[233] Omri Ben-Shahar and Ariel Porat, 'The Restoration Remedy in Private Law' (2019) 118 Columbia Law Review 1901, 1933-1935.

[234] Hannah R. Sullivan and Scott J. Schweikart, 'Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?' (2019) 21 AMA Journal of Ethics 160, 163-165.

preclude full autonomy in cases where there is a potential for significant harm.

3. Insurance-based solutions

A few thinkers suggest compulsory insurance schemes for AI systems, the way automobile insurance is compulsory for cars. This method spreads risks among stakeholders as well as paying compensation to persons affected by decisions made by AI. Insurance concepts can solve problems of compensation but might fall short in filling accountability gaps.

Insurance solutions are especially promising for meeting the compensation aspect of AI liability, providing victims with prompt redress without the need for lengthy lawsuits to determine fault[235]. The no-fault accident compensation scheme in New Zealand has been mentioned as an example that could be followed, as it already pays compensation for injuries without requiring evidence of negligence, a model that could be readily extended to injuries caused by autonomous systems.

The deployment of the insurance model is confronted with challenges, most notably relating to risk evaluation of new AI uses. Historical data is used by traditional actuarial techniques to price premiums appropriately, but data is limited for new AI technologies. A few jurisdictions have experimented with innovative solutions to this challenge, such as the United Kingdom's consideration of a temporary state-sponsored insurance regime that would be in place until enough data are available to enable private insurers to price AI risks accurately. This solution recognizes that liability insurance markets can fail initially because of information gaps while establishing a transitional system that safeguards innovation and possible harms.

In addition to compensation, insurance mechanisms can serve regulatory purposes through differential premiums, inducing economic incentives for risk reduction. Specialized insurance pools for AI developers in an industry might require technical standards and best practices as a condition of coverage, thereby instituting a private regulation complementing government strategies. Japan's recent revision of its Product Liability Act openly invites the creation of specialized insurance products for autonomous systems, acknowledging their potential role within an integrated liability framework.

---

[235] Japanese Ministry of Economy, Trade and Industry, 'Interpretative Guidelines on the Product Liability Act for AI-Based Products' (METI Guidelines, June 2022) Section 4.3

IV. A Hybrid Framework

This paper suggests a hybrid liability framework combining aspects of both frameworks to address their respective shortcomings. This framework comprises three key elements:

1. **Tiered liability based on system autonomy:** The standards of developer liability should be strengthened as AI autonomy rises, mirroring the diminishing role of human intervention[236].
2. **Explanation and disclosure obligations:** Developers must be more responsible for harms inflicted by "black box" factors that they cannot reasonably explain or document.
3. **Actions of user contribution:** Liability proportionally must decrease when users bypass security measures, misuse systems, or disregard documented boundaries.

This framework acknowledges that AI liability cannot be effectively addressed through binary assignment but requires a nuanced approach that reflects the distributed nature of AI development and deployment.

A. Autonomy-Based Liability Scaling

The first factor acknowledges that the level of liability must be different depending on the extent of autonomy being demonstrated by the AI system. For very autonomous systems that have little human control, developer liability correctly rises as the causal contribution of human operators diminishes. This solution provides a continuum of liability instead of an ad hoc categorization, enabling courts to determine where specific systems are located from human control to complete autonomy.

Instating this feature will involve the establishment of objective criteria by which to quantify autonomy, and these might include the following: the degree to which operational decisions are taken in the absence of human intervention, the ability of the system to learn about novel situations,[237] and the temporal length of isolated operation. Legal standards can be graded proportionally, from negligence-based standards for systems with high levels of human control to ones approaching strict liability for completely autonomous applications functioning in high-risk areas.

---

[236] Karni Chagal-Feferkorn, 'Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers' (2019) 30 Stanford Law & Policy Review 61, 86-89.

[237] Ellen Goodman and Julia Powles, 'Urbanism Under Google: Lessons from Sidewalk Toronto' (2019) 88 Fordham Law Review 457, 498-500.

B. Explainability as a Liability Mitigation

The explainability aspect tackles the "black box" issue that makes classical understandings of predictability problematic. By making liability incentives for transparency, this methodology incentivizes developers to invest in interpretable AI designs and sound documentation habits. Although complete explainability will continue to be technically challenging, this mandate acknowledges that developers can reasonably be expected to know and document the limitations, training parameters, and possible failure modes of their systems.

Courts implementing this approach will assess explainability across both technical and communicative dimensions. Technical explainability will assess whether developers have used appropriate methods to understand the operation of their systems, while communicative explainability will assess whether this understanding has been effectively conveyed to users in a way that enables informed risk assessment. Liability exposure will be correspondingly reduced for developers who demonstrate diligence in both dimensions.

C. User Responsibility Integration

The third element recognizes the active agency that users exercise in putting AI systems into particular use cases. Through the incorporation of comparative fault principles, this approach avoids disproportionately attributing blame to developers when users intentionally disable security measures or put systems beyond their intended uses[238]. It seeks to balance innovation incentives and consumer protection while also acknowledging that AI systems are situated within socio-technical systems where human decisions heavily shape outcomes.

The evaluation of user contribution encompasses the following factors: compliance with documented operational procedures; reaction to system warnings or confidence indicators; proper oversight depending on the degree of autonomy of the system; Alterations to default settings that impact safety margins. This method aligns with evolving international standards, including the IEEE 7000 series, which stress the obligation of organizations implementing AI systems to provide proper implementation and oversight.[239]

---

[238] Meg Leta Jones, 'The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216, 230-232.
[239] IEEE Standards Association, 'IEEE 7000-2021 - IEEE Standard Model Process for Addressing Ethical Concerns During System Design' (2021).

D. Practical Implementation Path

This hybrid framework will be implemented through concerted effort in legislative, regulatory, and judicial spheres. Laws can define foundational liability rules, while regulatory bodies formulate technical standards for autonomous measurement and explanation needs of various application areas.11 Courts will finally interpret these rules to particular cases, establishing a precedent that assures more certainty for developers and consumers.

Several jurisdictions are already trending in the direction of elements of this hybrid model. The EU's AI Liability Directive contains elements of disclosure obligations and tiered responsibility by risk category, and Japan's AI Governance Guidelines place an emphasis on requiring proper human monitoring proportionate to system capability.[240] Drawing from these nascent models, albeit adding express provision for consideration of user responsibility, the suggested structure provides a model solution to the attribution problem finding equilibrium between innovation and accountability.

V. Practical Implications

The new framework entails broad changes to current tort theories. Courts would have to come up with standards of measuring the autonomy of AI and acceptable explainability. Regulatory agencies must come up with documentation standards and certification protocols for high-risk AI uses.

For professionals, this framework will demand fuller risk evaluations and documentation techniques.[241] Contracts would be necessary to clearly establish responsibility between actors in the chain of AI development and deployment.

1. Challenges of judicial implementation

Courts will need to establish new judicial skills to evaluate the technical features of AI systems in implementing this framework. Sophisticated questions regarding the autonomy of systems and the reasonableness of explanatory measures must be evaluated by judges and juries without being victimized by hindsight bias. This challenge can be met by specialized courts or the incorporation of technical advisors into judicial processes, as have been developed for patent litigation or complex

---

[240] European Commission, 'Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence' COM(2022) 496 final; Japanese Ministry of Economy, Trade and Industry, 'AI Governance in Japan Ver. 1.1' (2023) 45-48.

[241] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701, 1736-1738.

scientific evidence. A number of jurisdictions, such as the Daejeon District Court in South Korea and the Technology and Construction Court in the UK, have already initiated specialized training programs for judges dealing with AI-related cases.[242] The evidentiary challenges are equally significant. Conventional discovery procedures can be insufficient for evaluating sophisticated AI systems, particularly where proprietary algorithms or distributed training procedures are used. Courts must establish protocols for digital forensics tailored to machine learning systems, such as demands for thorough logging of training data sources, hyperparameter choice, and deployment settings. These demands must strike a balance between transparency and valid intellectual property protections to prevent stifling innovation through overbroad disclosure requirements.

2. Regulatory Architecture

Efficient enforcement necessitates certain regulatory designs that complement classical judicial remedies. A multi-level regulatory design could involve pre-market certification for high-risk uses, regular monitoring obligations, and reporting mechanisms for incidents like those in pharmaceutical regulation. These kinds of frameworks would function optimally through collaborative modes of governance among technical standard-setting organizations, industry players, consumer groups, and government agencies to provide technical viability and public accountability.

Global coordination is especially problematic, with diverse regulatory strategies fragmenting markets and providing opportunities for arbitrage across jurisdictions. Organizations like the OECD and the Global Partnership on AI have started to develop agreed standards, but major differences still exist between leading jurisdictions.[243] The suggested framework can be enhanced by creating international standards for quantifying autonomy and explainability through current standards organizations like ISO or IEEE to ensure cross-border convergence while enabling proper local adaptation.

3. Industry adaptation

For AI developers and deployers, this framework will require significant changes in development and documentation practices. “Privacy by design” principles need to be complemented by “liability by design” approaches that integrate risk assessment throughout the development lifecycle. This

[242] Claire Park and Zoe Yi, 'Developing Judicial Capacity for AI Disputes: A Comparative Study' (2024) 18 Law and Technology Review 134, 151-154.
[243] Organisation for Economic Co-operation and Development, 'Recommendation of the Council on Artificial Intelligence' OECD/LEGAL/0449 (2019).

will include expanded testing regimes specifically designed to identify potential liability exposures, documentation protocols that capture design decisions related to unpredictability determinations, and improved communication mechanisms to communicate limitations and risks to downstream users.

Contractual arrangements need particular attention, with well-defined responsibilities along the AI value chain. Compensation methods based on conventional approaches can be insufficient where multiple actors are involved in a system whose behavior arises from their joint inputs. Novel contractual frameworks might involve proportionate liability provisions tied to individual system functions, dynamic compensation structures that adapt to degrees of system autonomy, and obligatory information exchange provisions that facilitate effective risk assessment for all involved.

4. Insurance Market Evolution

Insurance markets will have to create advanced actuarial models for AI risk, factoring in technical metrics on explainability, test coverage, and autonomy levels into premium calculations. New, specialized insurance products will arise across various segments of the AI value chain, such as developer professional liability insurance, deployer operational risk policies, and end-user abuse protection.[244] These new specialty products will enhance the liability model by converting abstractions in the legal risk of AI into determinable financial considerations that organizations will be able to integrate into business planning.

The implementation of this framework would involve a period of transition uncertainty and possible market disruption as stakeholders learn. A phased implementation strategy would enable courts, regulatory bodies, and industry players to build the required capabilities while ensuring adequate predictability for continued innovation. This might involve first application to high-risk areas with incremental extension, temporary safe harbours for good faith compliance efforts, and regulatory sandboxes permitting controlled experimentation with liability models.

VI. Conclusion

With increasingly complex artificial intelligence (AI) systems that start acting with degrees of autonomy as high as or even greater than the autonomy of human agents, conventional legal theories of responsibility and liability come under severe constraint. These systems, with independent decision-making capabilities and the ability to learn from

[244] Sean Griffith, 'Corporate Governance in an Era of Compliance' (2016) 57 William & Mary Law Review 2075, 2123-2125.

their surroundings, strain conventional fault and foresight conceptions. In such a case, it is critical that the legal frameworks catch up not merely with technological advances, but also to deal with the unprecedented risks and harms that could be incurred. This transformation must involve reconsidering core principles of tort and contract law, particularly insofar as liability for autonomous acts conducted by non-human actors is concerned.

The hybrid liability approach set out in this article aims to balance on a knife edge the need to promote technological innovation and ensure proper accountability. On the one hand, overly onerous liability legislation will inhibit research, development, and implementation of AI technologies. On the other, weak legal controls will result in major harm for individuals, businesses, and governments alike without due redress. The strict liability elements – whereby liability is applied independently of fault – and the control doctrine – both recognize the AI operation complexity – enable qualitative judgment of fault with consideration given to the technical construction and human direction involved within the particular scheme.

Finally, this hybrid model presents a more flexible and just legal framework that can embrace the distributed and frequently invisible character of decision-making in AI systems. It encourages legal certainty through the definition of precise standards of accountability, while also accepting that liability for AI-induced accidents may be distributed among designers, programmers, deployers, and even end users. In so doing, it sets the stage for a future jurisprudence that not only fills current legal gaps but also can accommodate future developments in AI. The key to such a framework is its flexibility and responsiveness to new developments while being committed to the underlying legal values of fairness, justice, equity, and public safety.

Reinforcing Legal Safeguards Against Deepfakes: Examining India's Regulatory Approach

- **Kabir Kumar***

Abstract

A key challenge in the intersection of law and technology is the legal system's persistent struggle to keep pace with rapid technological advancements. Deepfake technology—primarily powered by generative adversarial networks, as discussed in this article—highlights this ongoing challenge and offers valuable insights for academics and policymakers seeking to develop robust and enforceable regulations. By analyzing how Indian courts address deepfake-related claims under publicity rights, this paper advocates for a harm-centric approach to regulating deepfakes, emphasizing the need for stronger legal measures to mitigate their consequences. In conclusion, the paper calls for greater collaboration between legal and computer science experts to ensure that deepfake regulations are technically viable, comprehensively address potential harms, and, above all, remain enforceable.

I. Introduction

Photo and video-editing techniques and image manipulation have a history that is nearly as old as the concept of photography itself. The first 'hoax' photograph was produced two years subsequent to the creation of the first photograph. Taken by Hippolyte Bayard in 1840, this ‘fake’ image was a staged self-portrait that pictured Bayard slumped against a wall, meant to convey his disdain at not having been recognised as the pioneer of photography – a recognition he believed he was entitled to. Computer Graphic Imagery (CGI), Photoshop, and other such tools for visual media alteration have abounded in the creative arts for decades. Therefore, the issue of doctored imagery is not really a recent phenomenon and has been in conscious thought as long as media itself has existed. Yet recent instances of manipulated media flooding online channels of communication raise worrying concerns.

While these technologies have historically only been accessed by a select few in the creative arts industry, now, with the ever-burgeoning growth in computing technology, access to such technologies has become democratised and rather ubiquitous. The new smartphones launched by tech giants in recent years boast of AI-assisted camera technology. These AI enhancements could be as simple as enhancing the colour contrast of an image or as stark as removing unnecessary objects from a particular shot in order to reflect the aesthetic that the photographer truly had in mind. There are several photo and video-editing apps that are available to

* 2nd year BBA LL.B. student at O.P. Jindal Global University, Sonipat.

download from online application stores, most of which are either free to use or charge a minimal subscription fee. The democratized public access to such techniques and the innovation of new technologies like generative adversarial networks (the most common outputs of which can be deepfakes – image, video, audio, or text) means that more people can engage in media manipulation, in what can be said to be a regulatory void. In the current state of affairs, there is very little, if any, regulatory guidance as to what constitutes appropriate media manipulation with no harmful consequences.

Prima facie, there seems to be no problem with allowing people to edit media on their own. It can rather be seen to facilitate their expressive capabilities. However, as is often the case in free speech jurisprudence, the pursuance of an expanded right to freedom of expression of one person is met with its natural corollary - an affront or objection to such speech by another. This conflict is particularly apparent when we consider deepfake technology within the broader set of media manipulation techniques. A deepfake, in particular, is arguably far more harmful than a piece of text-based hate speech because of the potential the former has to spread misinformation and harm various stakeholders involved in the deepfake. How, then, can we reconcile the harms of such technology against the benefits it offers (if any) to the creative arts industry and free speech/innovation in general? This paper aims to discuss the current legal response to deepfakes in India, examine its drawbacks, and suggest a change in perspective in the hope that this re-evaluation will better redress the harms of deepfake technology.

II. Deepfakes

A. What are Deepfakes – The Technology and its Pros and Cons

Deepfakes are highly realistic, AI-generated media and are based on the technology of generative adversarial networks (GAN), which rely on deep learning AI algorithms. GANs consist of two convolutional neural networks (CNNs) that are pitted against each other (or are made adversaries). Each CNN is trained with examples of real images, which are run through them as training data, with the aim of enabling the system to categorise pictures, videos, and other data highly accurately. The data entered into the system is abstractly conveyed to the algorithm at the upper tiers of the neural network. After a significant quantity of images is input into the network—initially necessitating hundreds but now achievable with fewer than ten—the algorithm autonomously trains to classify images according to the similarity of their abstractions. Once the CNN is trained to recognise and categorize objects, the algorithm can be inverted. The mathematical operations are inversed, and an output is specified. As a result, an image is produced by the network based on the abstract features it has learned in the first stage of training. The initial CNN, which is trained to recognise

and categorise images, is called a detector, while the second inverted CNN is called the generator. Linking the two creates an autoencoder or a GAN. Pitting two such CNNs against

Each other forms the basis for the creation of a Deepfake. The generator CNN and discriminator/detector CNN are trained on the same data set, and while the first creates images/samples, the second discards all those which aren't similar to the original data set – i.e., it filters out those outputs which do not seem real. Working in this manner, the GAN produces hyperrealistic images and videos.

Although the first deepfake is said to have emerged in 2017, out of a Reddit thread under which a user anonymously posted pornographic videos created by GAN technology, and a 2019 DeepTrace study found that 96% of the deepfakes circulating the internet at the time were pornographic in nature, non-consensual intimate imagery is not the only use case of deepfake technology. Deepfakes, in the seven years (at the time of writing in 2024) since their emergence, have been created and used for several beneficial uses as well. They have been used in the advertising and retail industry for e-commerce virtual trial rooms, and even to personalise celebrity endorsements of local brands using a generic template. Deepfake technology has been used in the healthcare industry to train imaging and scanning technology. Making use of deepfake technology can avoid the cost and effort of having to re-shoot an entire film sequence because of a minor videographic error, and on a larger scale can even prevent the halting and restarting of filming in case of the untimely death of one of the actors. Deepfakes can also be used more generally for entertainment purposes, as creative expressions of unique ideas. There are several users across social media who create and distribute deepfakes and other types of AI-generated imagery and clips for purely artistic reasons and entertainment value.

Yet, deepfakes have an arguably more dangerous side to their nature. Based on the statistics mentioned above, the majority of the deepfakes circulating online channels of communication are pornographic in content, predominantly featuring the non-consensual sexualisation of women targets. Celebrities and non-celebrities alike have not been spared from the threats of non-consensual image abuse in the form of such deepfakes – which unfortunately may never be reported and may go unnoticed by the represented subject online. Moreover, audio deepfakes have been used to successfully defraud individuals and businesses out of large sums of money. Worryingly, deepfakes have also begun to be used in politics, in election campaigns, spreading propaganda and misinformation and generally curating a misleading narrative of political truth. A robo-call imitating the voice of US President Joe Biden was made to several voters in New Hampshire, urging them to avoid going to the electoral booths and dissuading them from casting their votes. The very threat of deepfake presence online threatened democracy in Gabon13 when President Ali

Bongo's sudden appearance in a public address after a prolonged period of absence was assumed to be a deepfake trying to cover up the fact of his supposed death. This triggered unrest and chaos and eventually a military coup to take over what was a presumed state of political instability.

Arguably, the biggest problem of deepfake technology that sets it apart from traditional forms of mis/disinformation is that a) deepfakes can be posted online anonymously, and their origin can be extremely difficult, if not impossible, to trace; and b) deepfakes are not easily verifiable for their authenticity. Receiving a piece of text-based vaccine misinformation on your WhatsApp need not raise a similar level of concern because it can be checked/verified against an established body of truth/scientific knowledge. However, how does one (a) recognize that an image/video/audio they have received is a deepfake and (b) verify its authenticity? There exists no centrally approved database in which all deepfakes are stored once they are created for us to verify whether the media we are consuming is the truth or a distorted reality purporting to be the truth. Nor do we have efficient detection technologies integrated into downstream channels of media consumption, which enable us to technically determine the AI-generated nature of a Piece of information we consume. In a regulatory void, especially in a country like India, the harms that deepfakes pose have been left to be addressed by courts. The lack of legislative basis for claiming injury against a harmful deepfake means that courts and judicial decisions, for the time being, are the most authoritative commentary we have on the redressal of these harms. Various courts and judges have come to differing conclusions on what constitutes an actionable deepfake harm, which forthcoming sections examine and elaborate on.

B. Deepfake Harms – A primer to the argument

A deepfake, in essence, is a distorted portrayal or an altered version of reality. It need not necessarily be based on a proven falsehood, but at its core, it is a piece of information that is fake. A deepfake is something that 'did not happen. ' The advantages and creative potential of influencing the media are limitless in entertainment and the arts; nevertheless, the drawbacks and dangers become clearer when examining deepfakes within the framework of societal institutions such as Democracy and Media.

The primary victims of a malicious, non-consensual deepfake would be the individuals depicted in the deepfake. Individuals have a plethora of remedies available against the contravention of the diverse interests they may have in a deepfake video. However, in addition to the loss of personal autonomy (of the individual subject(s)) that may come about as a consequence of synthetically altered media, there are other harms that could be brought about by the creation and distribution of a deepfake. There could be consequences felt by a collective of people – for instance, a particular race/caste/minority could be portrayed in prejudicial ways, or

certain sections of the larger audience viewing a deepfake might be specifically affected by the deepfake's message/impact. A racially biased deepfake video might affect the electorate's opinion on a suitable political representative. Similarly, politically microtargeted deepfakes might only be broadcast to certain sections of the larger populace, which will consequently affect the opinions, deceive, target, and/or confuse only that sub-sect of the population. Moreover, there also exists an intangible and perhaps unmeasurable impact on an audience bigger than a targeted collective – the society at large.

This could be different and varied depending on the nature of the content in the deepfake. A political deepfake could have cascading effects on trust in democracy and perhaps even the institution of media/information/knowledge. A pornographic deepfake could not only impact the represented individual but have important implications on the contours of what we determine to be rights to human dignity, reputation, and bodily integrity.

Deepfake harms, it is argued, occur on two levels simultaneously with every iteration of a deepfake of a natural person distributed to the public. These are at a) the individual level, the harm for which targets the subject of the deepfake, and b) the societal level, where the harm is felt by either the audience receiving/viewing the deepfake and/or by public institutions more broadly. Therefore, any regulation or legal decision that aims to address the 'harms' of deepfakes will ideally need to consider solutions that account for both levels of harms and adequately respond to them by adopting varying combinations of legal and technical safeguards against such harms.

III. Deepfakes and the Law in India

Globally, deepfakes have begun to gain some legislative and regulatory recognition. In the US, there are legislations regarding certain types of deepfakes. Some states (California and Texas) have regulations that curb the creation, dissemination, and use of pornographic deepfakes, while others (Virginia) have rules on the use of deepfakes in election campaigning. In contrast, the EU approach feels a bit more comprehensive. The EU AI Act represents a significant advancement in the regulation of deepfakes and generative AI technologies that can produce detrimental outcomes. The EU AI Act employs a risk-based framework, categorizing deepfakes as a 'limited-risk' technology, mandating that all online-shared deepfakes be marked or labeled in accordance with the transparency duties placed on deployers and providers of general-purpose AI models. However, there are no specific deepfake laws in India Ideally, this should have been covered under the recent Digital Personal Data Protection (DPDP) Act of India, passed in August 2023. Founded on the notions of individual 'dignity' and

'autonomy', the Right to Privacy in India has been operationalized through the DPDP Act to confer and safeguard individual privacy against private actors. However, the Act does not make any mention of deepfakes or related technologies and applications, which leaves much of the harm to be redressed by the courts of law. Judge-made decisions and rules guide the framework for remedies against deepfake harms, which have their own drawbacks and will be discussed ahead. Since deepfakes can be used to various ends, the harms they result in can be brought under different existing legal structures – a defamatory deepfake might invoke defamation laws (e.g. S 356 Bharatiya Nyaya Sanhita 2023), a fraudulent deepfake might come under S 318 of the Bharatiya Nyaya Sanhita, and a non-consensual pornographic deepfake might invoke penalties under S 294(2)(a) and/or S 79 of the Bharatiya Nyaya Sanhita, or the Indecent Representation of Women (Prohibition) Act of 1986. However, these legal recourses exist only when the deepfake causes harm in the relevant context. A general objection to the use of one's image and likeness without consent in a context that may not be sexual in nature or fraudulent in intent does not give rise to an adequate ground for a cause of action against such use. Much of the judicial discussion of deepfakes has tended to situate such harms within the jurisprudence of publicity rights and IP laws in the absence of a dedicated statute/legislation that addresses the specificities of deepfake harms.

A. A survey of Indian deepfakes

Narayana Murthy, Ratan Tata, Rana Ayub, Sachin Tendulkar, Manoj Tiwari, Alia Bhatt, Jackie Shroff, Anil Kapoor, Rashmika Mandanna, Aamir Khan, Ranveer Singh, Katrina Kaif and Kajol have more in common than just being famous Indian celebrities and well-known public figures. All of them have been represented in unauthorised deepfakes which have gone 'viral' on social media in the recent past. Apart from the first four individuals, all the others are popular Bollywood stars, who already have a large fan-following and can be considered influencers of public opinion in their own right.

Prior to examining the evolution of the legal response to deepfakes, it is prudent to investigate the types of damage arising from the deepfakes involving the aforementioned individuals. I have chosen to discuss five female and eight male celebrities, sampled from various arenas of public life – Narayana Murthy and Ratan Tata from the world of Business, Rana Ayub from Journalism, Sachin Tendulkar from Sport, Manoj Tiwari from Politics, and the remaining eight (four men and four women) from Bollywood (or Indian Cinema).

At this point, I want to draw the reader's attention to a disturbing fact that irrespective of the nature of the industry the female celebrity hails from, the deepfake made of her is pornographic in nature, or at the very least,

sexual. Rana Ayub's pornographic deepfake was made to scare her or warn her against publicly commenting on her political leanings. Alia Bhatt has been deepfaked twice with the first deepfake showing her making obscene gestures, and the second showing her dressing up and applying make-up. Rashmika Mandanna's face was deepfaked onto the body of a British Influencer and the focus was on the sexual nature of her clothing. A still image of Katrina Kaif from the movie Tiger 3 was morphed to show her scantily clad in a towel. Kajol's deepfake showed her changing outfits as part of the online get- ready-with-me (GRWM) trend.

Let us now consider the deepfakes of the male celebrities mentioned above. Narayana Murthy and Ratan Tata were purported to be endorsing trading apps and giving fake investment advice respectively in their deepfakes. Sachin Tendulkar was seen to endorse and praise a gaming app in his deepfake. Manoj Tiwari's deepfakes were versions of his political campaign speech in Haryanvi and English (with the content being the same as the original in Hindi), aimed to appeal to a more diverse voter base – arguably an example of a beneficial use of deepfake technology. Anil Kapoor claimed the misappropriation of his voice, image, and likeness in AI generated GIFs, emojis and videos, some of which satirically represent him in different movie posters, or showed him endorsing brands he has not endorsed. Jackie Shroff claimed remedies against several instances of misappropriation of his voice, image, and likeness, on merchandise, posters, etc., but the relevant claim to discuss here is perhaps against a video which shows him singing something using profane language, thereby harming his reputation. Lastly, both Ranveer Singh and Aamir Khan had deepfakes made of them in the run-up to the 2024 Elections, wherein it seemed they were asking people to vote for the Congress Party. All the 'male' related deepfakes are clearly harmful and constitute an affront to the represented individual's reputation, goodwill, credibility and right to privacy in terms of their opinions (political views) and economic interests (endorsements). However, none of these constitute an affront to their bodily integrity and dignity in the same manner as a pornographic deepfake video does, against the women mentioned previously.

The harm against a deepfaked woman's reputation, identity and bodily integrity at first glance, therefore, seems very different than an equally relevant but differently angled reputational, identity/autonomy and bodily integrity harm against a male target. While the trend of female-targeted deepfakes (based on the chosen sample, and also more generally) seems to veer towards non-consensual pornographic content, male-targeted deepfakes seem to focus more on appropriating the man's thoughts, opinions, and public persona/representation.

B. The right to publicity in India

The right to publicity emanates from the right to privacy. However, while privacy primarily deals with dignity infringements, publicity is a property-based right that encompasses damages which go beyond basic dignity harms of no-consent. Publicity rights deal with damages that arise out of commercial appropriation of identity. Publicity rights interestingly are available to celebrities and non-celebrities, although only the former can avail effective enforcement because of the commercial value associated with their identity. The publicity right is distinct from the right to privacy in that it attaches an economic value to the appropriation, and aims to restore the commercial 'disadvantage' that celebrities face when they do not give their consent. In the EU, publicity rights have been read into the Right to Privacy. In the UK, an individual's image draws protection under tort law – remedies are available under a breach of confidence and passing off. Perhaps the most developed jurisprudence on personality rights is from the jurisdiction of the US – unsurprisingly so, as the right to privacy emerged there with its first public reference found in the Warren and Brandeis' seminal paper on privacy rights in 1890. In 1903 , New York State acknowledged the right to safeguard against the unauthorized exploitation of an individual's name and likeness, marking the initial judicial recognition of the right to publicity, as established in Haelan Laboratories.

At present, given the lack of a deepfake specific legislation/regulation in India, courts and scholars seem to be veering towards addressing deepfake harms under the jurisprudence of publicity law. The right to publicity in Indian jurisprudence has undergone several iterations over the years. While there is no explicit law on the same, Indian courts derive their understanding of publicity protection under Articles 19(1)(a) and 21 of the Indian Constitution, (freedom of expression and right to life) and also draw inspiration from the spirit of IP laws in India. The Delhi High Court in Titan Industries gave us the definition of what it is to be a celebrity and held that an unauthorised, identifiable and commercial use of a celebrity's identity need not be accompanied by an element of deception, but rather is protected prima facie under the right to publicity. Building upon this case, Shivaji Rao Gaikwad broadened the contours of this right and held that even a reference to a person's name or likeness, when done so disparagingly or with derogatory connotations (akin to what is seen in a claim of defamation or damage to goodwill/damage of reputational harm in a claim of passing off) can be protected against by reading such damage as falling within a celebrity's right to a life of dignity under Article 21. In DM Entertainment the Court used the logic of trademark dilution to explain how commercial misappropriation of a celebrity's endorsement rights could confuse the public and therefore 'dilute' the celebrity's unique personality. Yet, in Gautam Gambhir also decided using a trademark lens, the Court asked for evidence of disrepute or confusion, in order to prove

that personality rights had been infringed (in stark contrast to the ratio of Titan Industries).

More recently, courts have tended to discuss the right to livelihood as a basis for protecting one's commercial identity, as seen in Anil Kapoor and Jackie Shroff both of which were decided over the past year (2023-24) and both of which included deepfakes within their claims. In Anil Kapoor the Court granted the plaintiff blanket protection against the deepfakes and other fake image/video endorsements that showed him supporting brands he did not, in reality, endorse. It was held that "the celebrity's right of endorsement would in fact be a major source of livelihood for the celebrity, which cannot be destroyed completely by permitting unlawful dissemination and sale of merchandise such as t-shirts, magnets, key chains, cups, stickers, masks, etc. bearing the face or attributes of their persona on it without their lawful authorisation." However, the same right to livelihood was discussed in the Jackie Shroff case, and an opposite conclusion was arrived at. The impugned video, in that case, was a compilation of interviews in which Jackie Shroff was forthright and witty, with an edit at the end of each statement superimposing emojis/clip art of black sunglasses, blingy jewelry, etc. Here, when the plaintiff claimed that these edits were disparaging and derogatory to his reputation, the Court disagreed and grounded this dissent in the balancing of the defendant's (a YouTube content creator) right to free speech and creative expression against a blanket right over one's image/persona. The Court opined that not only was such content creative and could not be stifled, but it also provided a source of income/livelihood and generated employment opportunities for a significant youth population.

This balance in favour of content creation is tricky because it tries to balance a right to free speech against a right to reputation that needs to be reasonably and objectively assessed regarding harm by including a layer of economic benefit of such free speech. The balance of the two rights has often been intended on a more principled level (freedom of thought, opinion and views on one hand versus the protection of dignity on the other), and by including the economic element of content creation, it may be seen as unfairly tilting the advantage in favour of the right to free speech. The test to determine harm to reputation is fairly objective already, and by expanding what would not amount to harm, we might end up with a narrower protection of reputation that could be argued as already unfair (as judicial treatment already considers objective determination of a subjective experience). By drawing on the right to livelihood as a basis for protection of one's personality, the Court contradicts itself in the two cases - Anil Kapoor's right to livelihood wins him protection against the creator's right to economic interests out of the misappropriation of identity, while it is reversed in Jackie Shroff's case, with no real legal basis for the distinction. However, more significantly, reliance on the right to livelihood also draws attention away from the fact that in both cases, the use of the

celebrity's identity was unauthorised and, therefore, had to be held liable. Adopting the perspective of Consent might make for more consistent judicial decisions on the right to publicity. A fairly simple dignity claim has been made more complicated than it needs to be by adopting a right to livelihood inquiry into the contours of the personality/publicity right. Therefore, the publicity rights jurisprudence in India at present seems messy without the application of a singular principle across the board.

C. The Harms that Case Law Fails to Capture

Indian publicity rights cases only seem to be concentrating on the individual harms that the misappropriation of identity causes against the celebrity who is claiming a remedy. The focus in these cases seems to be to provide a stronger sense of control over one's identity as the primary way to then combat unauthorized use of likeness – which, when extended to deepfakes, can cover non-consensual uses as well. This is ineffective when we consider building a response to deepfake harms, because not only does this perspective grant expansive rights over image and personality and might end up stifling free speech but it also implies that a deepfake gives rise to a cause of action only when the subject of the deepfake claims a remedy against it. However, more importantly, by focusing on the individual harms of unauthorised use of one's identity, the publicity law jurisprudence in India fails to take into account the societal implications of such unauthorised use in terms of deception. This lacuna is evident when we transport a publicity rights lens into the deepfakes enquiry.

The men represented in deepfakes surveyed in the above section equally face several individual level harms against their reputation, privacy, and dignity. Over the past year, with publicity rights jurisprudence growing out of the judgements in favour of Amitabh Bachchan, Anil Kapoor, and Jackie Shroff, we now have a legal description of these harms in the various publicity law cases that have been judicially pronounced. This allows us to legally label these harms as harms to their reputation, economic interests and livelihood, credibility, infringement of privacy, and misappropriation of their persona/identity. Yet what these judgements and judicial discussions fail to capture is an equal (if not more severe) harm that these very deepfakes cause the audience consuming them. This societal level harm emanates out of deception, misleading misrepresentation, and distortion of an objective truth. An individual-focused publicity rights regime that requires the affected individual to claim a remedy also means that deepfakes, which might mislead and deceive the general public (but are not brought to the notice of the concerned individual), may never be punished for the lack of a remediable harm. Taking this further, if the individual represented in the deepfake does not personally feel uncomfortable with the representation, but it nonetheless deceives a

receiving audience as to its truth, the deepfake may never be seen as infringing in any sense.

From a sociological point of view, deepfake harms against women in India (considering the celebrity deepfakes to represent the general populace, given that non-celebrity deepfakes are hard to identify, let alone turn viral) seem to not only be against the individual represented in the deepfake (in terms of an affront to her right to privacy, bodily integrity and dignity), but also comment on the harms against women in general as a sexualised species. Interestingly, and something that's arguably lamentable, is that none of the individual harms faced by women have received legal scrutiny and judicial declaration. Though there are sociological studies and papers that discuss the risks of deepfakes and the harm they can cause, as already mentioned, the current legal discourse doesn't adequately capture these societal-level harms that deepfakes pose. We also regrettably do not have judicial discourse on what these individual level harms (and consequent societal level harms) could be for women – because none of these women so far have successfully claimed injury before a court of law. Nor do we have a non-celebrity woman approaching a court of law for a judicial decision on what these individual harms can be legally described as. The subjective reputation of what it is to be a woman in India is not something that we have legal discourse on, and the downstream repercussions on what a deepfake can mean to an ordinary woman's reputation in her society/community do not seem to be discussed sufficiently enough. And it will continue to be disregarded as long as the lens we adopt in the law is one of deepfakes causing only 'individual level' harms and such harms being discussed and authoritatively remedied in the favour of male claimants.

IV. Enforcement

Given the seriousness of the negative objectives (most significantly, threats to human dignity and public institutions like democracy) that deepfakes can be created and used for, it is relevant to talk about a legal framework that can address the various harms emanating from such uses. Discussing deepfakes in India requires not only reframing our approach towards understanding what the different kinds of resultant harms are but also involves actively thinking about how we can go about enforcing remedies against such harms. The main argument in this paper has been to establish that deepfakes have multi-levelled harms emanating from them and that to redress deepfake harms, we need to consider the individual and societal interest together in order to build a legal framework that can do so effectively. The current preference to find the solution within the publicity rights discourse does not adequately achieve efficient redressal, and therefore, we might need to consider other remedies.

Apart from building a publicity rights regime to respond to the harms that deepfakes pose – which arguably is itself inadequate because it fails to account for the equal and simultaneous harm on the societal level- some scholars have chosen to explore intellectual property laws and the recourse they can offer. A lot of the pornographic deepfakes on the internet are similar to revenge porn cases. As in the latter, if the deepfakes are created using copyrighted images (most likely selfies that the represented women themselves have taken and therefore own a copyright over), copyright infringement laws can kick into application and help provide a legitimate cause of action to take down the infringing videos/images. However, this solution presupposes copyright ownership in the deepfake subject/individual and does not provide as much of an effective remedy if the ownership vests in an unrelated third party. A copyright-based remedy also fails to cover individual harms that are experienced by those 'identifiable' in a deepfake. While publicity rights might help cover those who are identifiable from the deepfake (even if the claimant is not the intended target but looks similar and is therefore, has a valid cause of action against the use of their likeness), copyright fails on this front because not only does it exclude targeted claimants (i.e., those that the deepfake creator intended to represent) who do not own a copyright in the training data, but it also ignores claimants who might be identifiable in the image/video (despite not being the intended target). Furthermore, copyright remedies are mostly based on a notice-and-takedown model. This requires the copyright holder to ask for the infringing use of the copyright to be enjoined and, very rarely, compensated. The limitation of such remedies being ex-post in nature suggests that even once ownership thresholds are met, copyright might prove insufficient in terms of mitigation measures and fail to adequately address the deepfake's harms to the claimant's tainted reputation and dignity. Moreover, a single takedown notice would also not prevent malicious deepfake creators/distributors from re-uploading the deepfake on a different website.

In addition to finding appropriate jurisprudence to even discuss what kinds of remedies accrue to deepfake harms, we need to go one step further in establishing how such remedies can be enforced. It can be argued that deepfakes harm (individual and societal) once caused are irreparable – a reputation once destroyed in a deepfake cannot then be redressed via compensation, nor can a loss of trust due to the deepfake's deception be regained through any viable means. In light of this argument, then, enforcement against deepfake harms, or the regulation of deepfakes, should consider ex-ante measures instead of merely relying on ex-post remedies, as the current laws around the world focus on. In the UK, this is being considered in a proposal to criminalise the very creation of deepfakes – therefore targeting the point of origin in order to prevent downstream harms emanating from its distribution and consumption. How this creation is to be targeted and enforced against is something that

we are still waiting to hear from lawmakers. However, other measures like deepfake detection as a part of content moderation and watermarking/labelling AI-generated content to facilitate informed consumption in downstream channels might help build a more robust enforcement framework when we are considering the development of a holistic legal response to deepfake harms. Any law framed to incorporate such ex-ante measures will have to be technically accurate and specific enough to ensure that such measures cover the redressal/prevention of harms that ex-post measures might not be able to adequately capture within their ambit. An interesting tool to facilitate legal notice of deepfake harms in India is the proposed bystander clause in the IT Rules, whereby anyone who encounters illegal content can impugn it. In the context of deepfakes, this would give rise to a cause of action against something that one finds or suspects to be a deepfake, even though they might not be represented in it themselves.

V. Conclusion

On the 25th of July 2024, the Oversight Board released its decision overturning Meta's original decision not to take down a deepfake of an Indian public figure. Meta had initially failed to take note of a user's notice and subsequent appeal regarding content that was pornographic. After the user appealed to the Oversight Board, Meta determined that it had left the post up in error and took it down as a violation of its Bullying and Harassment Community Standard. A similar case was reported where a female American politician was depicted as being groped, and she took it down immediately. This was then appealed to the Board by the user who had posted it. The Oversight Board's decision in both matters is clubbed into one, where both images were found to be violative of Meta's policies (in particular, with a recommendation to move such non-consensual sexualised manipulated media to the Adult Sexual Exploitation Community Standards from the Bullying and Harassment Policy), and Meta's initial decision to keep the post up in the Indian case was overturned, and its decision to take down the post in the American case was upheld. Meta's reason for not acting in the Indian case was that there were no news reports on the matter, and therefore, Meta did not have conclusive evidence that the impugned content was, in fact, a deepfake.

This is relevant for multiple reasons. First, it draws attention to the fact that in the absence of regulation that mandates platform behaviour with respect to deepfakes, self-regulation by such platforms is the only way deepfake harms can currently be addressed. Second, such self-regulation is inconsistent and often stands on shaky ground, either because the legal principles informing decisions are not objective and standard enough or because the platform does not need to satisfy public law principles of equality and non-discrimination or follow the rule of law. Third, the law

(self-regulation or otherwise) needs to catch up with technical advancements in the field – deepfake detection algorithms need to be integrated into platforms' content moderation obligations so as to facilitate their determination of AI-generated content. Relying on newspaper or media reports, as in Meta's first case, is dangerous for it is not only subjective and requires territorially contextual knowledge (which is difficult for a multinational corporation headquartered in the other side of the world), but also ignores the fundamental fact that most deepfakes out there are created of people who do not have a public presence/are not celebrities.

This paper is an attempt to discuss the harms posed by deepfakes and how the current legal response to them is inadequate and flawed. The primary argument asks for a re-evaluation of the structure of harms we consider resulting from deepfakes and using this perspective to inform how laws must be framed to respond to such harms in a way that is effective and enforceable. As the current legal response to deepfakes exists in India, it is predominantly publicity-oriented and, unfortunately, not expansive enough to cover all potential harms that deepfakes can cause. Technology is only becoming more sophisticated with the passing of time, and reports of an arms race between generations and detection abound in the tech industry. Moreover, the technology works across borders and results in harm across jurisdictions as well. The legal response to such harms cannot be territorial alone, and each jurisdiction will need to engage in active conversation with others in order to achieve standardised legal responses to the same legal harms that exist across the borders of countries. The law needs to consider incorporating responses that take into account the technical specificities of deepfake technology. Lawmakers, academics, and legal practitioners need to work together to build a deepfake-specific legal regime so as to cover all the harms that this technology is capable of while also recognising its potential to be put to beneficial use and facilitate creators' freedom of speech and expression.