DEEPFAKE TECHNOLOGY AND CYBERCRIME: A CRITICAL ANALYSIS OF THE INADEQUACY OF THE INFORMATION TECHNOLOGY ACT, 2000

Mohit Kumar B.A. LL.B., NMIMS Kirit P. Mehta School of Law, Mumbai

ABSTRACT

The accelerated development of artificial intelligence has resulted in the development of deepfake technology, which facilitates the production of highly realistic but fake audio, video, and visual content. Although this technology has many useful applications, its increasing misuse has been a major factor in the development of cybercrimes such as identity theft, financial fraud, non-consensual sexual material, and political misinformation. In the Indian context, cybercrimes are governed by the Information Technology Act, 2000, which was enacted at a time when technologies such as artificial intelligence-driven deepfakes were not even remotely possible. This paper critically evaluates the effectiveness of the Information Technology Act, 2000 in dealing with cybercrimes committed using deepfake technology. Adopting a doctrinal research methodology, the paper examines the relevant statutory provisions, judicial reactions, and enforcement difficulties under the existing legal regime. The paper contends that the current legislation is still fragmented, reactive, and inadequate to address the distinct legal and evidentiary challenges arising from deepfakes. The paper also undertakes a short comparative examination of the international regulatory regimes and proposes legal and policy reforms to enhance the Indian response to deepfake-enabled cybercrime. The paper finally reiterates the imperative need for a specific and proactive regulatory regime to address the challenges arising from artificial intelligence in the digital age.

Keywords: Deepfake Technology; Cybercrime; Artificial Intelligence; Information Technology Act, 2000; Digital Evidence; Privacy Law; Intermediary Liability.

1. INTRODUCTION

The increasing pace of development in digital technologies has brought about a paradigm shift in the production, distribution, and consumption of information. Artificial intelligence has become one of the most impactful technological advancements in the twenty-first century, transforming different sectors such as communication, governance, finance, and law enforcement. Although artificial intelligence has numerous advantages, its misuse has led to the development of new and sophisticated cybercrimes. Deepfake technology is one such form of cybercrime, which has the ability to produce realistic digital information that can mislead people as well as institutions. The growing use of deepfake technology for malicious purposes has raised serious concerns about privacy, reputation, democracy, and cyber security, especially in countries where legal development has not kept pace with technological advancements.

1.1 Background of Artificial Intelligence and Emerging Technologies

Artificial intelligence can be defined as the capability of computer systems to carry out tasks that require human intelligence, such as learning, problem-solving, and decision-making[1]. In the last ten years, there has been rapid growth in machine learning and data analytics, which has led to the development of AI technologies. These new technologies have greatly impacted digital media, making it possible to create content automatically, manipulate images, and generate voices. Even though these technologies have been used for legitimate purposes in learning, entertainment, and research, they have also been used to commit complex cyber crimes. However, the law has been unable to keep up with the rapid technological advancements**.**

1.2 Meaning and Evolution of Deepfake Technology

Deepfake technology is an artificial intelligence application, specifically deep learning, which enables the manipulation or creation of audio-visual material to misrepresent an individual as saying or doing something when they actually did not[2]. The term "deepfake" is a combination of the words "deep learning" and "fake," which indicates the reliance of the technology on neural networks to produce synthetic materials that are very similar to

[1] Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach (4th ed. 2021).
[2] Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753 (2019).

real ones. Deepfake technology was originally developed for research and entertainment purposes but has developed at a rapid pace and become widely available through open-source software and mobile apps. This has led to the potential for abuse because anyone with basic technical knowledge can now create deceptive digital material that can cause serious legal and social harm.

1.3 Rise of Deepfake-Enabled Cybercrimes in India

In recent years, there has been a substantial rise in cybercrimes in India that have been aided by new technologies such as deepfakes[3]. Deepfake crimes vary from identity theft and online impersonation to financial fraud, non-consensual pornography, and political disinformation. The application of deepfakes to manipulate video and audio files has made it difficult to distinguish between real and fake digital evidence. These crimes not only affect individuals but also affect the trust of the public in digital platforms and democratic institutions. The current framework of cybercrime law enforcement in India is challenged by the task of detecting and prosecuting deepfake crimes.

1.4 Need for Legal Regulation of Deepfake Technology

The abuse of deepfake technology reveals the existence of major loopholes in the existing legal system for cybercrime regulation in India. The Information Technology Act, 2000, which is the major legislation for the regulation of electronic crimes, was introduced when the concept of artificial intelligence-based technologies like deepfakes was not even on the horizon.[4] As a result, the Act does not have any direct provisions for the generation, distribution, and misuse of synthetic media content. The Act's provisions are usually made use of in an indirect manner, resulting in difficulties in enforcement. The lack of a dedicated legal system not only makes deterrence difficult but also makes the protection of basic rights like privacy, reputation, and freedom of expression challenging.

1.5 Scope and Objectives of the Study

The research scope will be restricted to the study of the legal challenges that arise from deepfake technology under the Indian cybercrime laws. The research will concentrate on

[3] National Crime Records Bureau, Crime in India 2022 (Ministry of Home Affairs, Government of India).
[4] Information Technology Act, No. 21 of 2000 (India).

the analysis of the legal adequacy of the Information Technology Act, 2000 in dealing with deepfake technology-assisted cybercrimes, apart from other relevant provisions of the Indian Penal Code. The research aims to achieve three different objectives: first, to comprehend the nature and effects of deepfake technology as a cybercrime tool; second, to critically assess the current legal framework that regulates such crimes in India; and third, to provide recommendations for legal and policy interventions to improve India's response to the challenges of deepfake technology in the digital era.

2. CONCEPTUAL FRAMEWORK OF DEEPFAKE TECHNOLOGY

2.1 Meaning and Nature of Deepfake Technology

Deepfake technology can be defined as the application of artificial intelligence to create or manipulate digital content in a manner that misrepresents a person's image, voice, or behaviour. By employing sophisticated computational methods, deepfakes can create the illusion that a person has made a statement or engaged in an activity when, in fact, they have not. The hallmark of deepfake technology is its capacity to generate highly realistic and believable synthetic media, which can easily fool a casual observer and make it difficult to distinguish between real and fake content[5].

The nature of deepfake technology is rooted in its deceptive capabilities. Unlike other digital manipulation technologies, deepfakes are based on machine learning algorithms that improve with each exposure to large amounts of data. This results in content that is modeled on human behaviour, speech patterns, and physical movements. Because of its realistic nature, deepfakes raise serious concerns about reputation, privacy, and the authenticity of digital content.

2.2 Technological Basis of Deepfakes (Artificial Intelligence and Machine Learning)

The main technology used in deepfakes is based on artificial intelligence and machine learning algorithms. These algorithms are trained on a large set of data, including pictures, videos, and audio recordings of people. Based on patterns identified in this data, the technology is trained to create fake facial expressions, voice tones, and body movements. Over time, the technology

[5] Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753 (2019).

is able to create new content that looks and sounds authentic, even though it is all artificial.

One of the main technologies that power deepfakes is deep learning, which relies on multi-layered neural networks to analyse information. These networks increase their accuracy levels as more information is fed into them, making deepfakes even more believable and difficult to spot. The fact that such technology is now so easily accessible, through open-source platforms and mobile apps, has led to a high risk of misuse. This means that deepfakes are no longer the domain of experts but are available to the general public[6].

2.3 Types of Deepfakes (Audio, Video, Image and Text)

Deepfakes can be categorized into various types depending on the nature of the content they are manipulating. Video deepfakes are the most popular type of deepfakes, where the face or activities of a person are manipulated digitally to create misleading videos. Audio deepfakes are the type of deepfakes where a person's voice is cloned, which enables the creation of misleading statements or commands. Image-based deepfakes are the type of deepfakes where images are manipulated to create misleading photographs of people in compromising or misleading situations.

Recently, text-based deepfakes have also come into existence, where artificial intelligence is used to create written content that imitates the style of communication of a person. Each of these types of deepfakes poses a different challenge, especially when it comes to evidence and verification. The various types of deepfakes make it difficult to regulate their misuse, as each type of deepfake may be governed by a different law or may not be regulated at all[7].

2.4 Legitimate Uses versus Malicious Uses of Deepfake Technology

Despite the negative potential, deepfake technology is not necessarily illegal or unethical. There are many other legitimate uses of deepfake technology, such as in the film industry, education, healthcare, and assistive technology. For instance, deepfake technology can be applied to recreate historical figures for educational use, enhance dubbing in movies, or help people who have lost the ability to speak. In these ways, deepfake technology can be applied

[6] Ian Goodfellow et al., Generative Adversarial Networks, 27 Advances in Neural Information Processing Systems 2672 (2014).
[7] Ajder et al., The State of Deepfakes: Landscape, Threats, and Impact, Deeptrace Report (2019).

for constructive and socially positive purposes[8].

The negative application of deepfake technology has, however, raised serious legal and ethical issues. Deepfakes are increasingly being used for identity theft, online impersonation, financial fraud, non-consensual pornography, and political disinformation. These acts not only cause harm to individuals but also undermine public trust in online platforms and democratic institutions[9]. The challenge of distinguishing between legitimate applications and negative misuse of deepfake technology underscores the pressing need for legal frameworks and regulatory protections to ensure that the technology is not abused while still allowing innovation to proceed.

3. Deepfake Technology as a Tool for Cybercrime

Deepfakes have increasingly shown up as a potent tool in perpetrating cybercrimes. This is because deepfakes make it possible for a cybercriminal to create a convincing yet false digital image, which can be used to deceive and harm others. The use of deepfakes has widened the scope of cybercrimes and has posed a challenge to law enforcement agencies and the legal system in regulating cybercrimes.

3.1 Deepfakes and Identity Theft

Identity theft is one of the most prevalent types of cybercrimes that use deepfake technology. Deepfakes make it possible for cybercriminals to virtually impersonate a person by copying their facial features, voice, or behaviour. This impersonation can be used for unauthorized access to personal accounts, fooling people they know, or tricking digital identity verification systems. In most instances, the victim is not aware of the identity theft until the damage is already done.

The fact that deepfake content is realistic makes identity theft more complex and hard to track. Conventional measures like voice recognition or video authentication can be easily circumvented using deepfake content. This has severe legal ramifications, as current identity theft legislation was not intended to cover highly advanced impersonation methods made

[8] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2021.
[9] Robert Chesney & Danielle Keats Citron, The Law of Deep Fakes, 82 Md. L. Rev. 1 (2023).

possible by AI technology[10].

3.2 Deepfakes in Financial Fraud and Online Scams

Deepfakes are also increasingly being employed in financial fraud and online scams. Perpetrators employ deepfakes to create audio or video content that can be used to impersonate company executives, business associates, or even relatives in order to deceive victims into handing over financial information or money. Online scams rely on trust and urgency, making them highly effective.

The employment of deepfakes in financial crimes has resulted in a blurring of the lines between traditional financial fraud and technologically enabled financial deception. Financial institutions and individuals have increasingly turned to digital communication for financial transactions, making them susceptible to deepfake-enabled impersonation. Current financial fraud laws cover general deception but do not address the specific risks associated with AI-generated synthetic media[11].

3.3 Deepfake-Based Non-Consensual Sexual Content

One of the most harmful uses of deepfake technology is the creation of non-consensual sexual content. Deepfakes are frequently used to superimpose the faces of individuals, particularly women, onto explicit images or videos without their consent. Such content is often circulated online with the intent to harass, humiliate, or extort victims.

The legal and psychological consequences of such misuse are severe. Victims suffer reputational damage, emotional distress, and social stigma, while legal remedies remain limited and slow. Although laws addressing obscenity and sexual exploitation exist, they do not adequately address the unique nature of deepfake-generated content, which often involves digitally fabricated material rather than real acts[12].

3.4 Political Manipulation, Misinformation and Threats to Democracy

Deepfakes are a threat to democratic processes because they can be used to disseminate

[10] Robert Chesney & Danielle Keats Citron, The Law of Deep Fakes, 82 Md. L. Rev. 1 (2023).
[11] Federal Bureau of Investigation, Public Service Announcement on Deepfake-Enabled Fraud (2023).
[12] Danielle Keats Citron, Sexual Privacy, 128 Yale L.J. 1870 (2019).

political misinformation. This can be done through the creation of videos or audio recordings of political leaders that are not genuine. These can be used to manipulate public opinion, cause unrest, or even create doubt about the electoral process[13].

The application of deepfakes in politics threatens the principles of democratic governance because it creates doubt about the authenticity of information. This is because, in such a scenario, it becomes difficult for people to make decisions based on information that is not genuine.

The law is not equipped to handle the issue of deepfakes because they can be used to disseminate information across borders.

4. Legal Framework Governing Deepfake-Related Cybercrime in India

The Information Technology Act, 2000, and the Indian Penal Code, 1860, are the major laws governing cybercrime in India. However, both laws were enacted prior to the development of artificial intelligence technology such as deepfakes. As a result, deepfakes are dealt with only indirectly by existing laws, leading to loopholes in interpretation and enforcement[14].

Section 43 of the Information Technology Act, 2000, deals with civil liability for unauthorized access to computer systems and misuse of digital data, which can be applied to deepfakes in some cases. Sections 66C and 66D of the Information Technology Act, 2000, pertain to identity theft and cheating by personation through computer resources, which are generally applied in cases involving the use of deepfakes to impersonate people for cheating. Sections 67 and 67A of the Information Technology Act, 2000, pertain to the publication and transmission of obscene and sexually explicit material in electronic form, which are generally applied in cases involving the use of deepfakes for non-consensual sexual content. However, these sections were enacted to regulate traditional cybercrimes and do not specifically regulate the creation and distribution of AI-generated synthetic media[15].

Certain sections of the Indian Penal Code, 1860 are also applicable to the harm caused by deepfakes. Sections that pertain to cheating by electronic means and defamation are applicable

[13] Bobby Chesney & Danielle Keats Citron, Deep Fakes and the New Disinformation War, Foreign Affairs (2019).
[14] Information Technology Act, No. 21 of 2000 (India); Indian Penal Code, 1860 (India).
[15] Information Technology Act, No. 21 of 2000 §§ 43, 66C, 66D, 67, 67A (India).

in cases where cheating and defamation are involved, while sections that pertain to voyeurism can be applied in cases involving sexually explicit deepfakes. However, the IPC is a general criminal code and does not have any specific provisions to address the use of fabricated identities or content[16].

The involvement of online intermediaries is a key factor in the proliferation of deepfakes. Section 79 of the Information Technology Act provides conditional immunity to online intermediaries for third-party content, provided they comply with due diligence obligations. However, this provision also means that digital platforms are not held accountable for the content, as action is only taken after the content is reported as unlawful. The lack of AI-specific obligations in the intermediary liability provisions also indicates that the current legal framework is inadequate to address deepfake-related cybercrimes[17].

5. Inadequacy of the Information Technology Act, 2000 in Addressing Deepfake Crimes

The Information Technology Act, 2000 was formulated in a scenario where the use of artificial intelligence to create synthetic media like deepfakes was not foreseen. Consequently, the Information Technology Act, 2000 lacks any statutory definition for the term "deepfake" or "synthetic media." This is a major source of ambiguity, as law enforcement agencies and the judiciary are left with the task of dealing with deepfake-related crimes in terms of provisions originally designed for other cybercrimes. The lack of a proper definition makes it rather difficult to uniformly categorize and prosecute deepfake crimes, thus undermining the efficacy of the legal framework[18].

The Information Technology Act also lacks in treating deepfake-related crimes as a separate category of crimes. The Information Technology Act, 2000 deals with identity theft, cheating, and publication of obscene content in general terms but fails to address the special nature of AI-related crimes. Deepfake crimes involve the use of automated content generation with very little human intervention, making it rather difficult to establish the mens rea or criminal intent. The legal standards for establishing criminal intent are not very helpful in crimes that cause harm through algorithmic means[19].

[16] Indian Penal Code, 1860 §§ 419, 420, 499–500, 354C (India).
[17] Information Technology Act, No. 21 of 2000 § 79 (India); Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[18] Information Technology Act, No. 21 of 2000 (India).
[19] Robert Chesney & Danielle Keats Citron, The Law of Deep Fakes, 82 Md. L. Rev. 1 (2023).

Jurisdictional and evidentiary concerns further highlight the challenges posed by the IT Act. Deepfakes can be produced, processed, and shared across different jurisdictions within seconds, often through anonymous or foreign-hosted platforms. The Information Technology Act does not offer much in terms of cross-border enforcement and international cooperation in such scenarios. Moreover, the evidentiary requirements to establish the authenticity or falsity of digital content produced through deepfake technology are quite challenging. This is because the judicial and investigative authorities may not possess the necessary technical know-how and forensic capabilities to detect manipulated content, thereby causing delays in adjudication[20].

The IT Act's provisions regarding the regulation of social media platforms and online intermediaries are also inadequate in the context of deepfake distribution. Although online intermediaries are provided with conditional immunity under the Act, their responsibilities remain largely reactive. This means that platforms only need to respond after being notified about the illegal content, allowing deepfakes to spread rapidly and cause irreparable harm before being removed. The lack of AI-specific due diligence requirements, such as the proactive identification or tagging of synthetic media, further hampers platform accountability[21].

In conclusion, the Information Technology Act, 2000 is a reactive and outdated piece of legislation when it comes to cybercrime regulation. The law is mostly reactive in nature and focuses on remedying the situation after the fact rather than taking a preventive approach that is technology-friendly. In the case of deepfakes, this is especially true because the pace, scope, and anonymity of AI-generated content require a more proactive and technology-friendly legal approach. This is proof that the current legal framework is not sufficient to deal with the challenges posed by deepfake technology.

6. Judicial and Comparative Perspective

The judiciary has a significant role to play in determining the legal treatment of new forms of cybercrime, even in the absence of legislative guidance. While Indian courts have not yet had the opportunity to adjudicate many cases involving deepfakes, judicial guidance on cybercrime, digital evidence, and privacy issues is an important starting point for understanding how cases

[20] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[21] Information Technology Act, No. 21 of 2000 § 79 (India); Shreya Singhal v. Union of India, (2015) 5 SCC 1.

involving deepfakes might be adjudicated.

In the case of Shreya Singhal v. Union of India, the Supreme Court of India highlighted the need to balance freedom of speech with regulation of online content and defined the scope of intermediary liability under the Information Technology Act of 2000. The Court held that intermediaries cannot be held liable for third-party information unless they have actual knowledge of its illegality. While this ruling is significant for protecting freedom of speech, it also points to the challenges of a reactive regulatory framework, especially in the case of deepfakes, where harmful content can go viral in a matter of minutes before any notice is even issued[22].

The judgment in the case of Anvar P.V. v. P.K. Basheer is important in the context of crimes related to deepfakes. The Supreme Court has established stringent guidelines for the use of electronic evidence, underlining the importance of authenticity and certification. In the context of deepfake technology, the authenticity of digital evidence becomes an important aspect. The guidelines established in this case highlight the challenges that courts may encounter in evaluating deepfake evidence without the aid of sophisticated forensic analysis[23].

Moreover, in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court established the right to privacy as a fundamental right under the Constitution. Deepfake technology challenges this right by facilitating the misuse of an individual's image, voice, and identity. Although this case does not address deepfakes, its focus on informational privacy establishes a constitutional foundation for regulating technologies that impinge upon individual autonomy and dignity[24].

From the comparative analysis, it is evident that different nations have begun to understand the risks associated with deepfake technology. In the United States, the regulation of deepfakes is still in its infancy, with different states beginning to draft legislation to mitigate the risks associated with the misuse of deepfakes in elections and non-consensual intimate images. However, there is no federal legislation governing deepfake technology in the United States.

In the European Union, there is a more comprehensive approach towards regulating deepfake

[22] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[23] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[24] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

technology through the proposed Artificial Intelligence Act. The EU framework lists high-risk AI systems, including those that have the capability of producing deceptive synthetic media, and makes them adhere to the principles of transparency, accountability, and risk management. The requirement for disclosure or labeling of AI-generated content offers valuable lessons to India on how to develop a proactive legal framework to address the risks associated with deepfakes[25].

7. Challenges and Way Forward

It is seen that the regulation of deep fake is posing challenges because of the pervasiveness of this technology in the changed scenario. Challenges in regulating deep fake technology include the gap between technology and law. Technology progresses at an incredibly fast rate, while legislation finds it difficult to keep up. Laws are made but are always seen as outdated as legislation is a slow process. Another instance of this is the Information Technology Act of 2000. The legislation was drawn up in an era when such technologies as artificial intelligence-based synthetic media did not even exist.

The other major problem that exists in the field of cyber law is the identification of deepfakes. As technology has evolved and artificial intelligence tools have gotten more sophisticated, it has become very difficult to distinguish between real and fake content. This makes the identification of deepfakes very hard for law enforcement agencies, and as such, the culprits get away due to anonymity.

In addition, freedom of speech issues contribute to the complexity of regulating deepfakes. Every attempt to control online content strikes the delicate balance required to control the regulation of offensive material without infringing upon the constitutional right to free expression. Excessive control will lead to censorship, while insufficient control allows offensive deepfake material to spread uncontrollably. This is the ongoing problem.

In the backdrop of these challenges, there is a need for several legal and policy interventions. The first of these is the need for a new legal framework in artificial intelligence, which can effectively explain the concept of deepfake technology and criminalize the misuse of this technology. This new legal framework can effectively enlighten all law enforcement and

[25] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2021.

judicial agencies. The other need is for several changes to be made to the IT Act of 2000, addressing new elements of artificial intelligence, along with better guidelines for liability.

Additionally, the role and responsibilities of digital platforms must be built upon through the concept of enhanced intermediary responsibilities. Social media sites must be made to include detection tools, identification of AI-created content, as well as timely removal of content that is deemed to be dangerous. Lastly, education and digital literacy can be crucial to mitigating the effects of deepfake content on society as a whole. Education can be focused on the general public as well as institutions to minimize the impact of the dangers of deepfake technology.

8. Conclusion

This paper has sought to examine the increasing misuse of deepfake technology as a means of cybercrime and critically evaluated the current legal framework that India has adopted to deal with the challenges that have been posed by the increased misuse of deepfake technology. Accordingly, this paper has highlighted the legal, social, and institutional risk associated with deepfake technology with a particular emphasis on its conceptual foundations, the various cybercrimes that have been facilitated via deepfakes, and the legal responses that have been adopted to deal with deepfakes.

The analysis above reveals that the Information Technology Act, 2000, is inadequate in such issues pertaining to crimes related to deepfakes. The lack of a definition of deepfakes, the lack of including crimes related to AI, issues in establishing criminal intention, issues related to evidence, and the regulatory challenges faced by online intermediaries in tackling the issue of deepfakes have resulted in a highly inadequate Information Technology Act, 2000. Although the judicial system tried to overcome digital crimes with the help of existing constitutional provisions and cybercrime laws, these measures were inadequate.

This essentially means that, with the rapid advancement in artificial intelligence technologies, India needs urgent legal reform. An update to the regulatory framework should be not only forward-looking but also sensitive toward technology in the wake of malicious use of deepfakes and striking a balance among innovation, free speech, and privacy. In the absence of timely legislative intervention, the existing legal framework will continue to remain ill-equipped in protecting individuals and institutions as well as democratic processes from the constantly evolving threats the technology has on offer.