DEEPFAKES: THREATS TO COMPUTER FRAUD AND SECURITY UNDER INDIAN LEGAL PROVISIONS

Neha Verma, Ph.D. Research Scholar, Royal School of Law and Administration, The Assam Royal Global University, Guwahati, Assam.

ABSTRACT

Deepfake technology, which utilizes artificial intelligence to create highly realistic fake videos, audio, and images, is rapidly becoming a tool for cybercriminals. In India, this technology is being exploited to facilitate various forms of fraud, including identity theft, financial scams, and social engineering attacks. These threats put individuals at risk and compromise the security of businesses and government systems. This paper examines how deepfakes contribute to computer fraud and security risks while exploring how Indian laws can address these challenges. Deepfakes allow criminals to impersonate people convincingly, making it easier for them to carry out fraudulent activities, like stealing money or spreading false information. These digital forgeries are particularly dangerous because they target systems that rely on facial recognition, voice authentication, and other forms of digital identity verification, which are now more vulnerable to manipulation by deepfakes. In India, laws like the Information Technology Act, 2000 (IT Act) provide legal tools to deal with cybercrimes, including fraud and identity theft linked to deepfakes. Sections 66C and 66D of the IT Act, for example, criminalize identity theft and impersonation, while the Indian Penal Code (IPC) also has provisions for cheating and fraud. Digital Personal Data Protection Act (DPDPA), 2023, which focuses on privacy and data protection, could also help regulate the misuse of personal data in deep fake content. However, the current legal system faces significant challenges in addressing these crimes, as deep fake technology evolves quickly and often outpaces law enforcement's ability to respond. This paper also examines the difficulties law enforcement faces in detecting deepfakes and suggests that better training, stronger laws, and more advanced detection technologies are needed to protect against these growing threats. The paper concludes by recommending that India enhance legal frameworks, raise public awareness, and adopt AI-powered tools to combat deep fake fraud and safeguard digital security.

Keywords: Deepfake Technology, Artificial Intelligence, Cybercrimes, Fraud, Security Systems.

I. INTRODUCTION

Deepfakes are an emerging global concern, including in India. They refer to manipulated or synthetic media, often produced using artificial intelligence (AI) techniques like deep learning, to create or alter videos, audio recordings, or images in a highly convincing way. These media can serve both harmless and harmful purposes. Deepfake technology relies on advanced algorithms to create hyper-realistic videos by mimicking a person's voice, face, or likeness through machine learning methods. The resulting fake videos or audio are altered to make it appear as though the person is saying or doing something they did not do.

Characterized by their remarkable realism, deepfakes are generated using AI applications that combine various technologies to craft a new audio or video clip. This process involves layering, altering, and merging images to create a complex, realistic final product. Deepfakes can take the form of face reenactment, face generation, face swapping, and speech synthesis. Face reenactment involves manipulating an individual's facial features, while face generation creates an entirely new face that is not linked to any specific person. Additionally, face swapping replaces one person's face with another's, and speech synthesis reconstructs voices.[1] Deepfake technology is a double-edged sword.[2] On the one hand, it has some exciting and creative potential. In entertainment, for example, deepfakes can be used in movies and TV shows to create realistic special effects or even bring historical figures back to life for educational purposes. In virtual reality and gaming,[3] it helps create more immersive and personalized experiences with lifelike avatars and interactive media. It also has valuable applications in education, where it can simulate real-world scenarios for training purposes. However, the dark side of deepfakes is especially troubling when it comes to digital fraud. Cybercriminals can use deepfake technology to impersonate people, like public figures or business leaders, by mimicking their voice or face, tricking others into sharing sensitive information or committing fraud. It can also be used to manipulate financial systems, such as creating fake videos of executives authorizing wire transfers or convincing employees to approve fraudulent payments. Beyond that, deepfakes can be used for highly convincing

[1] Shinu Vig, Regulating Deepfakes: An Indian Perspective, 17 J. Strat. Sec. 70 (2024), https://doi.org/10.5038/1944-0472.17.3.2245

[2]Karin Kelley, The Double-Edged Sword of AI Deepfakes: Implications and Innovations, Centre for Technology & Management, https://pg-p.ctme.caltech.edu/blog/ai-ml/double-edged-sword-of-ai-deepfakes-implications-innovations
(last visited Nov. 4, 2025).

[3] Carolina Cruz-Neira et al., Virtual Reality and Games, 2 Multimodal Technol. & Interact. 8 (2018), https://doi.org/10.3390/mti2010008

phishing attacks, where attackers impersonate trusted individuals to steal passwords or confidential information. In politics, deepfakes can create fake videos of politicians saying or doing things they never did, spreading misinformation, and damaging public trust. Even individuals can suffer, as deepfakes can be used to create harmful or defamatory content, ruining reputations and causing personal distress.[4] As technology advances and becomes more accessible, the risks of deepfake-related fraud only grow, making it essential to develop stronger detection tools, cybersecurity practices, and legal protections to prevent its misuse. The rise of deepfakes has caused significant concern as they can be used to manipulate public opinion by creating fake media, such as counterfeit political or explicit videos of individuals without their consent, potentially damaging their personal and professional lives. Although deepfakes may seem convincing at first, their widespread use has led to the rapid spread of false information.[5]

Deepfake technology is rapidly becoming a major concern for cybersecurity and fraud due to its potential to enable new and sophisticated methods for criminals to carry out harmful activities like identity theft and financial scams. One of the most concerning threats posed by deepfakes is identity theft.[6] With deepfake technology, criminals can create fake videos or audio that closely resemble real people, allowing them to impersonate someone else. This can trick victims into revealing sensitive personal information, such as passwords or financial details. The ability to mimic trusted individuals makes this a serious security threat, as it opens the door for fraudsters to access private data and cause significant harm to victims. Another critical issue is the use of deepfakes in financial scams.[7] Criminals can leverage deepfake technology to create convincing fake videos or audio of company executives or other high-ranking officials. By impersonating these individuals, they can deceive employees into authorizing money transfers, revealing confidential information, or engaging in other fraudulent activities. There have been documented cases where attackers used deepfake audio[8]

[4] Mullen, Molly 'A New Reality: Deepfake Technology and the World Around Us' Mitchell Hamline Law Review: Vol. 48: Iss. 1, Article 5.(2022). Available at: https://open.mitchellhamline.edu/mhlr/vol48/iss1/5
[5] Abdul-Rahman, Kabbara. "Bots & Deepfakes." NSI Intern Integration Project, August 2021. https://nsiteam.com/social/wpcontent/uploads/2021/08/IIJO_eIntern-IP_Bots-and-Deepfakes_Kabbara_FINAL.pdf.
[6] Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. ACM Computing Surveys, 54(1), 7:1-7:41. https://doi.org/10.1145/3425780
[7] Westerlund, M.. The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review, 9(11), 40–53. (2019) https://doi.org/10.22215/timreview/1282
[8] Goh, D. H.-L., Lee, C. S., Chen, Z., Kuah, X. W., & Pang, Y. L. (2022). 'Understanding Users' Deepfake Video Verification Strategies. In C.Stephanidis, M. Antona, S. Ntoa, & G. Salvendy (Eds.), HCI International 2022 – Late Breaking Posters pp. 25–32. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-19682-9_4

to imitate the voices of company directors, successfully convincing their targets to send substantial sums of money.

Beyond personal and financial threats, deepfakes also pose a significant risk to the spread of misinformation. The ability to create realistic yet entirely fake content, such as videos or speeches, can mislead the public, distort facts, and damage trust in online communications. This is particularly troubling in the context of politics, public health, and social issues, as deepfakes make it harder for people to discern what is true and what is fabricated.[9] The spread of such content can have far-reaching consequences for society, undermining trust in media and institutions. As deepfake technology becomes more advanced, the challenge of detecting these fakes grows more complex. The sophistication of deepfake videos and audio makes it increasingly difficult for organizations to spot them and protect themselves from associated threats. The growing prevalence of deepfakes highlights the urgent need for the development of more effective detection tools. These tools are essential in combating the malicious use of deepfakes and ensuring the security of individuals and organizations in the digital age.[10]

The purpose of this paper is to examine the risks that deepfake technology poses to computer security and fraud prevention in India. As deepfakes become increasingly sophisticated, they present significant threats to both individuals and organizations, enabling fraudsters to manipulate media and deceive people in harmful ways. This paper will also evaluate the existing legal provisions in India, assessing their effectiveness in addressing deepfake-related crimes such as identity theft, financial fraud, and defamation. By analyzing current laws and their application, the paper aims to identify potential gaps and propose improvements to enhance legal protections and combat the growing threat of deepfakes in the digital age.

1.1. AIM OF THE RESEARCH

This research aims to explore the growing threat of deepfake technology and how it impacts computer fraud and security, specifically in the context of Indian laws. The study looks into

[9] Gilbert, Chris & Gilbert, Mercy. 'The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation'. International Research Journal of Advanced Engineering and Science, ISSN 2455-9024. pp.170-181.(2024)

[10] Gilbert C. & Gilbert M.A.'The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges'. Global Scientific Journals.ISSN 2320-9186,vol.12(9),pp.427-441.(2024) https://www.globalscientificjournal.com/researchpaper/.

how deepfakes are being used for crimes like identity theft, financial fraud, and scams, and evaluates whether India's current laws are sufficient to deal with these new challenges. The research aims to highlight gaps in existing legal and security measures and suggest ways to strengthen them. Ultimately, the goal is to offer practical recommendations for improving detection, updating laws, and creating policies to better protect against deep fake-related fraud and ensure digital security in India.

1.2. METHODOLOGY

The methodology of this paper combines a comprehensive review of existing literature, legal analysis, case studies, expert interviews, and data analysis to examine the implications of deepfake technology on computer fraud and security within the Indian legal framework. Expert interviews with professionals in cybersecurity, law enforcement, and law will provide insights into current challenges and potential solutions. The paper proposes actionable policy measures and future research directions to enhance India's response to deep fake-related threats. The combination of qualitative and expert-driven analysis ensures a well-rounded exploration of the issue.

II. DEEPFAKE TECHNOLOGY AND ITS ROLE IN COMPUTER FRAUD

2.1. Understanding Deep Fake Creation and Usage

Deepfake technology is still in its early stages, with the underlying mechanisms for creating such content being relatively new and evolving. However, even at this stage, deepfakes have already made their way into various areas of society. While their most widespread use so far has been in the adult film industry,[11] deepfakes have also had an impact on politics, social media, and education. The potential implications of this technology continue to expand, presenting an overwhelming range of possibilities.[12] Deepfakes are created by taking the image or likeness of one individual and replacing it with that of another, using an AI-driven facial recognition algorithm. This process relies on deep learning, which is a branch of machine

[11] Karen Hao, Deepfake Porn is Ruining Women's Lives. Now the Law May Finally Ban It., MIT TECH. REV. (Feb. 12, 2021), https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-comingban/ [https://perma.cc/PV9M-CKCH]

[12] Kristen Dold, Face-Swapping Porn: How a Creepy Internet Trend Could Threaten Democracy, ROLLING STONE (Apr. 17, 2018, 8:47 PM), https://www.rollingstone.com/culture/culture-features/face-swapping-porn-how-acreepy-internet-trend-could-threaten-democracy-629275/ [https://perma.cc/AS7F-TQDB];

learning inspired by the brain's structure and function through artificial neural networks.[13] There are generally two primary methods for synthesizing deepfakes.

The first method for creating deepfakes involves using generative adversarial networks (GANs). This process relies on two GANs working together: one network generates an image based on a latent sample, while the second network evaluates whether the image is real or fake.[14] The second network continuously provides feedback, rating the authenticity of the image and making adjustments until the computer can no longer distinguish the fake image from the original.

An alternative method uses deep learning systems known as variational auto-encoders (VAEs). VAEs consist of two networks that are trained to encode an image into a simplified representation and then decode it back into an image. The decoder contains a database of images of a desired figure, such as a celebrity, which it adjusts until the generated image matches the input.[15] The decoder can also add features like hats or sunglasses. For example, to create a deepfake of the late President George Washington riding a Segway, one encoder would focus on identifying Washington's face, while the other would work with various other faces. After training, the output from both encoders would be combined, producing an image of Washington's face on another person's body, potentially engaged in humorous or sensational activities, like riding a Segway.

Deepfakes can be particularly challenging to identify as fake because they often incorporate real footage, and clear audio, and are widely shared across social media platforms like Twitter, Facebook, Instagram, and TikTok, reaching large audiences. Moreover, with the widespread issue of "fake news," deepfakes are likely to exacerbate the spread of misleading information in increasingly convincing forms. The impact of deepfakes can extend to virtually every aspect of daily life, including personal relationships, education, professional opportunities, politics, and the legal system. While there may be some positive applications for deepfake technology, as discussed later, their existence could lead to negative consequences if the public remains

[13] T. T. Nguyen, C. M. Nguyen, D. T. Nguyen, D. T. Nguyen, and S. Nahavandi, "Deep Learning for Deepfakes Creation and Detection," arXiv preprint arXiv:1909.11573, 2019.
[14] Ming-Yu Liu, Xun Huang, Jiahui Yu, Ting-Chun Wang, and Arun Mallya. Generative adversarial networks for image and video synthesis: Algorithms and applications. Proceedings of the IEEE, 109(5):839–862, 2021.
[15] Marissa Koopman, Andrea Macarulla Rodriguez, and Zeno Geradts. Detection of deepfake video manipulation. In The 20th Irish Machine Vision and Image Processing Conference (IMVIP), pages 133–136, 2018.

unaware of the potential risks. The legal field, in particular, needs to grasp the harmful and unethical behaviors that deepfakes can trigger.

2.2. Examples of deepfake content

Many deepfakes on social media platforms like YouTube and Facebook are seen as harmless fun or artistic creations featuring public figures, both living and deceased, there is also a darker side to the technology. This includes harmful uses like celebrity and revenge porn, as well as efforts to influence political and non-political matters. A lot of deepfakes target celebrities, politicians, and corporate leaders because photos and videos are abundant them available online, providing the necessary material to train an AI deepfake system. Most of these deepfakes are created for fun, serving as pranks, jokes, or satirical memes intended to entertain or amuse.[16]

Deepfakes have become a growing concern in India, with multiple celebrities falling victim to this advanced form of digital manipulation. One of the most notable instances involved popular actress Rashmika Mandanna. A deepfake video went viral, depicting her entering an elevator in a black yoga suit. However, it was soon revealed that the video was a digitally altered version of an original clip featuring social media influencer Zara Patel. This incident raised significant privacy concerns, as Rashmika Mandanna publicly expressed her discomfort with such deepfake content, highlighting the potential harm it could cause to individuals' reputations and privacy. The Indian government issued a reminder to social media platforms about the legal provisions and penalties associated with the creation and dissemination of deepfakes. This incident underlined the urgent need for legal and regulatory frameworks to tackle the growing misuse of deepfake technology, especially when it targets public figures.

Deepfakes have also affected other prominent personalities. Sara Tendulkar, daughter of cricket legend Sachin Tendulkar, revealed that fake accounts impersonating her had surfaced on platforms like X (formerly Twitter). In her post, she expressed her concerns about the misuse of technology and called for more trust and authenticity in online communication. Similarly, other celebrities like Priyanka Chopra, Alia Bhatt, and Katrina Kaif have been victims of deepfakes, with altered videos and images being circulated online. These instances highlight a broader issue where deepfake technology is increasingly being used not just for entertainment

[16] Mika Westerlund, 'The Emergence of Deepfake Technology: A Review', Technology innovation Management Review, vol.9 no.11. Pp. 43.(2019)

or political manipulation but also for commercial gain, as seen in the case of Tom Hanks, whose likeness was used without his consent in a deepfake advertisement for a dental plan.

The rise of deepfakes in India and globally has sparked a call for stronger regulation and enforcement, with many advocating for stricter penalties for those who create and spread such content. These concerns are not only about protecting the privacy of individuals but also about safeguarding the integrity of information in the digital age. As deepfake technology becomes more accessible and sophisticated, the challenge of detecting and preventing its misuse will only become more pressing, necessitating a collaborative effort from governments, tech companies, and public figures alike.

2.3. Types of Fraud Facilitated by Deep Fakes

Deepfake technology poses significant cybersecurity threats by enabling hackers to create convincing fake audio and video to impersonate individuals, including executives and public figures. These deepfakes are used in identity theft, fraud, vishing attacks, social engineering, extortion, and disinformation campaigns. They also facilitate corporate espionage and unauthorized financial transactions. The growing use of deepfakes highlights the need for stronger cybersecurity measures to combat these evolving risks.

Identity Theft and Fraud: Deepfake technology allows criminals to replicate someone's voice or face, enabling them to commit identity theft and fraud[17]. For instance, fraudsters use deepfake audio to engage in vishing (voice phishing), where they impersonate a company's CEO to authorize fraudulent transactions. The authenticity of these deepfake audios presents significant risks to businesses and financial institutions.

Social Engineering and Psychological Manipulation: Deepfakes are increasingly used in social engineering attacks, where realistic videos or images can trick individuals into becoming victims of extortion, blackmail, or the spread of harmful disinformation. The rise in political misinformation, where manipulated images or audio of politicians are used to sway public opinion or influence elections, highlights how deepfakes can undermine democracy and

[17] Koops, B.J. and Leenes, R.,. Identity theft, 'identity fraud and/or identity-related crime: Definitions matter'. Datenschutz und Datensicherheit-DuD, 30(9), pp.553-556, 2006

the credibility of the media[18].

Corporate Espionage and Financial Crime: Deepfakes are also used in corporate espionage, with companies becoming targets of fraud and disinformation. Criminals have used deepfake videos or voice calls to impersonate executives, authorizing unauthorized transactions that lead to significant financial losses[19]. This emphasizes the dangerous potential of deepfakes in the financial sector and the urgent need for robust security measures within companies to combat these threats.

Compromising National Security: Deepfakes pose a major threat to national security by facilitating advanced disinformation campaigns. Malicious actors can use this technology to spread false information, destabilize society, and potentially incite conflicts between nations. According to research, deepfake technology is seen as an "information apocalypse," as it enables the creation of manipulated media that can fuel political division or promote misleading stories. This makes it increasingly difficult for intelligence agencies to verify the authenticity of digital content and assess its reliability.[20]

2.4. Risks to Digital Identity and Verification Systems

Deepfake technology poses a serious threat to digital identity, particularly to systems that rely on biometric verification, such as facial and voice recognition. As AI and deep learning continue to advance, it's becoming easier to create highly realistic fake videos and audio recordings. This creates vulnerabilities in verification systems, making it harder to distinguish between real and manipulated content.[21] These deepfakes not only put individual identity security at risk but also raise privacy concerns, as malicious actors could exploit these weaknesses for purposes like identity theft or impersonation.

[18] Bhusal, Chandra Sekhar. "Systematic review on social engineering: hacking by manipulating humans." Journal of Information Security, vol. 12 pp. 104-114.(2021)
[19] Ruhl, Christopher A. "Corporate and Economic Espionage: A Model Penal Approach for Legal Deterrence to Theft of Corporate Trade Secrets and Propriety Business Information." Valparaiso University Law Review vol.33, no. 2 763-811.(2011)
[20] Chesney, Bobby, and Danielle Citron. "Deep fakes: A looming challenge for privacy, democracy, and national security." Calif. L. Rev. vol.107 pp.1753. (2019):
[21] Joseph Foley, 14 Deepfake Examples That Terrified and Amused the Internet, CREATIVE BLOQ (June 1, 2021), https://www.creativebloq.com/features/deepfake-examples [https://perma.cc/WH3E-RM9P].

2.4.1. Vulnerabilities in Face and Voice Recognition Systems

Face and voice recognition systems, which are increasingly used in everything from personal devices to government security applications, are particularly vulnerable to deepfake attacks. These biometric systems, initially designed to enhance security, have become prime targets for deepfakes capable of creating false representations of individuals. For instance, attackers can use deepfake videos to impersonate legitimate users, bypassing security measures.[22] Similarly, voice cloning technology allows fraudsters to convincingly mimic individuals during voice verification calls, further undermining the reliability of these systems[23]. As both deepfake technology and biometric recognition systems evolve, the need for stronger defenses against such threats becomes more urgent. Security systems must adapt rapidly to these emerging challenges to prevent exploitation.

2.4.2. Impact on Biometric Security in Banking, Government, and Other Sectors

The growing sophistication of deepfake technology has profound implications across various sectors, particularly banking and government. In banking, biometric verification methods such as facial recognition or voiceprints used to approve transactions are at significant risk of being bypassed by deepfakes.[24] This not only exposes individual customers to potential fraud but also threatens the integrity and trustworthiness of financial institutions. Similarly, in the public sector, biometrics play a critical role in identity verification for national security and other sensitive operations. Deepfakes pose a direct threat to these security measures, as they could allow unauthorized individuals to gain access to classified information or manipulate official records.[25] With deepfakes becoming more sophisticated, sectors such as banking and government must invest in advanced detection tools and countermeasures to protect their systems from manipulation and safeguard sensitive data.

2.4.3. Legal and Technological Safeguards

To address these growing concerns, it is essential to develop robust legal frameworks and

[22] Benjamin Goggin, From Porn to 'Game of Thrones': How Deepfakes and Realistic-Looking Fake Videos Hit It Big, BUS. INSIDER (June 23, 2019, 10:45 AM), https://www.businessinsider.com/deepfakes-explained-the-rise-of-fake-realistic-videos-online-2019-6 [https://perma.cc/XY6M-TUZK].
[23] Thomas P. Gallanis, The Rise of Modern Evidence Law, 84 IOWA L. REV. 499, 530 (1999).
[24] Venkatraman, Sitalakshmi, and Indika Delpachitra. "Biometrics in banking security: a case study." Information Management & Computer Security 16, no. 4, pp. 415-430.(2008).
[25] Ndaba, Nomkhosi Lucia. "The impact of government employees using biometrics in IT security management at KZN Treasury." PhD diss., (2019).

technological safeguards aimed at preventing the misuse of deepfake technology. Collaboration between technology developers, lawmakers, and policymakers is vital in creating comprehensive strategies that can protect digital identities and secure critical infrastructure from deepfake manipulation. This collaborative effort must focus on strengthening both the legal response to deepfakes and the technological tools needed to detect and counteract these threats in real time.[26]

Deepfake technology represents a rapidly evolving and serious threat to biometric security and digital identity verification systems. Addressing this challenge requires immediate action from security experts, lawmakers, and industry leaders. Innovation in both technological advancements and legislative measures will be essential to mitigate the risks posed by deepfakes and ensure the continued protection of vital sectors, such as banking, government, and beyond.

III. LEGAL PROVISIONS IN INDIA TO ADDRESS DEEP FAKE-RELATED FRAUD

The government is starting to recognize the growing threat of deepfakes and the wide-ranging impact they could have on various sectors of society. There is a growing concern that, as India continues to push for technological progress, the rise of more advanced deepfakes will be an inevitable consequence, spreading into different areas of society as technology evolves. At this moment, India doesn't have a specific set of laws to tackle this issue and is instead relying on existing laws like the Information Technology Act, 2000 (ITA), along with the general criminal provisions in the Indian Penal Code, 1860 (IPC), However, vide notification (S.O. 850(E)) by the Home Ministry in the official gazette, July 1, 2024 marks as the effective date for enforcement of the new Penal Code viz., the Bharatiya Nyaya Sanhita, 2023 (BNS),[27] replacing the IPC, about a sesquicentennial old law[28], Digital Personal Data Protection Act (DPDPA), 2023, Indian Copyright Act, 1957, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules.

[26] Mullen, Molly 'A New Reality: Deepfake Technology and the World Around Us,' Mitchell Hamline Law Review: Vol. 48 : Iss. 1 , Article 5. (2022) Available at: https://open.mitchellhamline.edu/mhlr/vol48/iss1/5
[27] Bharatiya Nyaya Sanhita, 2023, Law No. CG-DL-E-25122023-250883, Dec. 25, 2023,
[28] Bureau (2024). Three Criminal Laws To Be Effective From July 1. The Hindu. [online] 24 Feb. https://www.thehindu.com/news/national/three-newly-enacted-criminal-laws-to-come-into-effect-from-july-1/article67881602.ece. (Last Accessed: 25 February, 2024).

3.1. Information Technology Act, 2000 (IT Act)

The Information Technology Act, 2000 (IT Act) in India can provide legal protection and avenues for action against the misuse of deepfake technology in several ways:

Section 43: Penalty and compensation for damage to computer, computer system, and Data. This section of the Information Technology Act of 2000 pertains to unauthorized access to and damage to computer systems, networks, or data. This includes actions like hacking, introducing viruses, or accessing information without permission. The punishment under Section 43 is a civil liability for damages, which can extend to ₹1 crore or more, depending on the extent of the damage caused.

Section 66C: Identity theft: Section 66C of the Information Technology Act, 2000, deals with identity theft. It criminalizes the act of using someone else's identity or accessing their personal information without their consent, often with the intent to commit fraud or other illegal acts. The punishment for identity theft under Section 66C is imprisonment for up to three years, and one shall also be liable for a fine which may extend to ₹1 lakh.

Section 66D: Cheating by personation: Section 66D of the Information Technology Act addresses the crime of cheating by personation, which involves using deceptive means or pretending to be someone else to gain financial benefits or deceive another party, typically via electronic communication or online platforms. The punishment for cheating by personation is imprisonment for up to three years and a fine that may extend to ₹1 lakh.

Section 66E: Violation of Privacy: This deals with the violation of privacy by capturing, publishing, or transmitting private, intimate, or sexual images of someone without their consent. This includes the illegal use of personal information, photographs, or videos for harmful purposes. The punishment for violating privacy under Section 66E includes imprisonment for up to three years and/or a fine which may extend to ₹2 lakh.

Section 67: Punishment for Publishing or Transmitting Obscene Material in Electronic Form. This section criminalizes the publishing or transmission of obscene material in electronic form. This includes the distribution or sharing of sexually explicit content online, including pornography, via email, websites, or other digital platforms. First conviction: Imprisonment for

up to five years and a fine that may extend to ₹1 lakh. Subsequent convictions: Imprisonment for up to 10 years and a fine that may extend to ₹2 lakh.

Section 67A: Punishment for Publishing or Transmitting Obscene Material in Electronic Form (Sexually Explicit Content). Section 67A of the Information Technology Act, 2000, criminalizes the publication or transmission of sexually explicit content in electronic form. It specifically addresses the distribution or sharing of material that is deemed to be sexually explicit or obscene, such as pornography, via electronic platforms like websites, emails, or social media. First conviction: Imprisonment for up to five years and a fine which may extend to ₹1 lakh. Subsequent convictions: Imprisonment for up to ten years and a fine that may extend to ₹2 lakh.

Section 67 B: Punishment for Publishing or Transmitting Child Pornography. Section 67B specifically addresses the issue of child pornography in electronic form. It criminalizes the publication, transmission, or even possession of any child sexual abuse material (CSAM) in digital form. First conviction: Imprisonment for up to five years and a fine that may extend to ₹1 lakh. Subsequent convictions: Imprisonment for up to seven years and a fine that may extend to ₹5 lakh.[29]

3.2. Indian Penal Code (IPC)

The Indian Penal Code (IPC) provides a range of provisions that can help safeguard individuals and society from the harmful effects of deepfakes. Although the IPC does not specifically address deepfake technology, its various sections can be applied to cases involving impersonation, fraud, defamation, and other forms of harm that deepfakes may cause.

The Bharatiya Nyaya Sanhita, 2023 includes provisions for criminalizing the creation and distribution of fake or manipulated content, particularly when it is used to harm or defame others. Deepfakes, which involve the use of AI to create realistic but fake audio, video, or images, can be used to spread misinformation, manipulate public opinion, or cause reputational damage. The BNS 2023 aims to address the growing concerns around digital manipulation and the potential harm caused by deepfakes, with a focus on protecting individuals' rights, privacy, and security in the digital age.

[29] The Information Technology Act, 2000, No. 21 of 2000.

Various sections of the IPC can be applied to safeguard individuals from crimes related to deepfake technology.

Cheating by personation: Section 419 criminalizes "cheating by personation," which involves impersonating someone else with the intent to deceive or harm. Deepfake technology can be used to create false representations of people, making them appear as if they are saying or doing things they never did. If deepfakes are used to impersonate someone and cause harm or deceive others, this section can be applied to hold the perpetrators accountable for cheating by personation. The punishment for the offense includes imprisonment for up to three years, a fine, or both.

Wantonly giving provocation with intent to cause riot: Section 153 addresses acts that provoke public disorder or riots. Deepfakes could be used to create false videos or audio that incite violence, spread misinformation, or inflame public sentiment. In such cases, this section could be invoked to hold those responsible for using deepfake technology to stir unrest or harm social peace. The punishment for the offense includes imprisonment for up to one year, or a fine, or both.

Obscene Acts and Songs: Section 294 deals with obscene acts in public or the distribution of obscene material. Deepfake technology can be used to create videos or songs with sexually explicit or offensive content, potentially damaging the reputation and privacy of individuals. This section can be applied to prevent and punish those who use deepfakes for obscene purposes in public or private contexts. The punishment for the offense includes imprisonment for up to three months, a fine, or both.

Punishment for Forgery: Section 465 criminalizes forgery, which includes the creation or alteration of documents, signatures, or records with fraudulent intent. Deepfakes can be used to forge videos, audio recordings, or images of individuals, thereby misrepresenting facts or causing harm. This section can be invoked when deepfakes are used to create fraudulent representations with the intent to deceive others. The punishment for the offense includes imprisonment for up to two years, a fine, or both.

Defamation: Section 499 deals with defamation, which occurs when false statements are made about someone to harm their reputation. Deepfake technology can be used to create false videos or audio of individuals, which, if distributed, can damage their reputation. This section can be

invoked to prosecute those who create or spread deepfakes that defame others. The punishment for the offense includes imprisonment for up to two years, or a fine, or both.

Cheating and Dishonestly Inducing Delivery of Property: Section 420 criminalizes cheating and dishonestly inducing someone to deliver property. Deepfakes may be used in scams to deceive people into transferring money or property, such as by impersonating a trusted individual, like a CEO or family member. This section can be applied to prosecute those who use deepfake technology to commit financial fraud or scams. The punishment for the offense includes imprisonment for up to seven years and a fine.[30]

3.3. The Digital Personal Data Protection Act (DPDPA), 2023

The Digital Personal Data Protection Act (DPDPA), 2023, focuses on protecting people's data in the digital world and managing how it's used, especially with technologies like deepfakes. Deepfakes can manipulate a person's image, voice, or likeness without permission, which can lead to serious privacy issues. The DPDPA helps tackle this by giving individuals control over their data and providing guidelines for businesses and organizations that use personal data to create AI-generated content like deepfakes.

3.3.1. Impact on Deepfake Content and Privacy Violations

Consent (Section 6): The DPDPA requires that individuals must give clear consent before their personal data is used to create deepfakes. Without consent, creating or sharing deepfake content is against the law.

Right to Access and Correction (Section 17): People have the right to see what personal data is being used about them and can ask for corrections. If their likeness or voice is used in a deepfake without permission, they can request to have it corrected or removed.

Right to Erasure (Section 21): If deepfake content is made without consent, individuals can ask for it to be taken down from online platforms, ensuring their personal data used in deepfakes is deleted if misused.

[30] The Indian Penal Code, 1860, Act No. 45 of 1860, enacted by the Parliament of India, received the assent of the Governor-General on October 6, 1860. It was published in the Gazette of India.

Data Minimization and Purpose Limitation (Section 5): The Act stresses that only the minimum amount of personal data necessary for a specific purpose should be collected. This helps reduce the risk of deepfakes being created by limiting the amount of personal data available for misuse.

Data Fiduciaries' Accountability (Section 24): Organizations that handle personal data must ensure it's protected. If deepfakes are created using someone's personal data, those responsible (data fiduciaries) must ensure it's used legally and put safeguards in place to prevent misuse.

3.3.2. Regulatory Approach to Managing Misuse of Personal Data in AI-Generated Content

The DPDPA also provides a structured approach to managing the risks of deepfakes and AI-generated content:

Data Protection Impact Assessment (Section 25): Organizations creating deepfakes or AI-generated content must assess the risks to privacy before using personal data. This helps identify and address potential issues early.

Penalties for Non-Compliance (Section 30): There are strict penalties for businesses or individuals who misuse personal data to create deepfakes without permission. This helps prevent data abuse by providing consequences for non-compliance.

Transparency and Accountability (Section 24): Organizations must be open about how they use personal data, making their processes for creating AI-generated content, including deepfakes, clear to the public. They must also be held accountable for any violations.[31]

3.4. The Copyright Act, 1957

The Copyright Act of 1957 of India primarily safeguards the rights of creators and owners of original works, including literary, artistic, musical, and cinematographic creations. While the Act was not designed specifically to address deepfakes or cyber fraud, it can still protect in certain contexts where deepfake content involves the unauthorized use of copyrighted materials, such as an individual's image, voice, or other artistic works. In such

[31] Ministry of Electronics and Information Technology (MeitY), Government of India, The Digital Personal Data Protection Act (DPDPA), 2023, No. 61 of 2023, published in the Gazette of India.

cases, the Act can serve as a tool to fight back against the exploitation of copyrighted content within deepfakes.

Section 13 of the Copyright Act, ensures protection for artistic and literary works. If a deepfake video uses copyrighted works like an individual's image or voice without permission, it can be considered an infringement. In this case, the creator or rights holder of the work can claim that their rights have been violated under the Act. This provision protects against unauthorized manipulations of copyrighted content, such as those commonly seen in deepfake videos.

Furthermore, the Copyright Act grants creators the exclusive right to reproduce their works under Section 14. This means that no one can create derivative works, such as deepfake content, from the original work without the creator's consent. If a deepfake uses someone's image, voice, or other artistic works without permission, the original rights holder can claim that their reproduction rights have been violated. This helps prevent the misuse of personal images and voices in fraudulent or harmful deepfake content.

The Copyright Act also provides remedies for infringement under Sections 51 and 55. If a deepfake content creator uses copyrighted works without authorization, the copyright holder can take legal action to stop the infringement. Remedies can include an injunction (to prevent further use), damages, or even criminal penalties if the infringement is intentional. This offers a legal route for individuals whose images, voices, or other copyrighted materials are misused in deepfakes for fraudulent activities, such as identity theft or financial fraud.

In addition to protecting the economic rights of creators, the Copyright Act also safeguards moral rights under Section 57. These include the right to attribution and the right to the integrity of the work. If a deepfake manipulates or distorts a person's image or voice in a way that harms their reputation, it could infringe on their moral rights, especially if the content is copyrighted. In such instances, the individual could seek legal action for the violation of their moral rights under the Act.[32]

The provision mentioned above does not directly address the issue of AI-generated content or the specific challenges posed by deepfakes. While it can be applied when copyrighted material is involved, it does not inherently tackle issues related to personal data, privacy, or consent that

[32] The Copyright Act, 1957, Act No. 14 of 1957, enacted by the Parliament of India, received the assent of the President on May 11, 1957. It was published in the Gazette of India.

are central to deepfake technology. These concerns may be better addressed by other legal frameworks, such as the Digital Personal Data Protection Act or anti-cybercrime legislation.

IV. OBSERVATIONS

Observations regarding the legal landscape surrounding deepfakes, privacy violations, and protection:

1. Deepfake technology presents serious risks to privacy and security, as it can be used for harmful purposes like identity theft, fraud, and spreading false information. However, current laws are not fully equipped to handle these challenges.

2. Existing laws like the Information Technology Act and the Indian Penal Code focus on issues like fraud and defamation, but they don't directly address AI-generated content such as deepfakes. This leaves significant gaps in protecting against deepfake-related crimes.

3. India does not yet have a specific law or regulatory framework to deal with deepfakes. The current legal system cannot fully address the unique and complex problems posed by this technology.

4. While the Copyright Act, of 1957 can protect against the unauthorized use of copyrighted material in deepfakes (such as images or voices), it does not cover broader issues like obtaining consent or protecting personal privacy in these cases.

5. The Digital Personal Data Protection Act (DPDPA), 2023 offers guidelines on data use, including consent and data minimization. However, it still needs updates and improvements to better handle the specific challenges deepfakes present.

V. CONCLUSION AND SUGGESTIONS:

SUGGESTIONS:

To better address the challenges posed by deepfake technology, this paper puts forward several key recommendations aimed at strengthening the legal, technological, and societal framework in India.

1. India needs to update its laws to specifically tackle deepfakes, setting clear rules and penalties for creating and spreading AI-generated fake content. A law focused on deepfake technology would fill the current gaps in the legal system and help address this new challenge.

2. Law enforcement also needs better training and resources to effectively identify and investigate deepfake crimes. Officers must understand how deepfakes work and learn to use AI-powered tools to detect them.

3. Public awareness is key in fighting deepfakes. Education campaigns should teach people how to spot deepfakes and the risks involved, so they can protect themselves from becoming victims of fraud.

4. Collaboration between lawmakers, tech developers, and industry leaders is key to creating these solutions for this emerging issue.

5. Additionally, India should invest in advanced AI tools that can detect deepfakes more accurately. By partnering with tech developers, law enforcement can create stronger detection systems that keep up with the fast-paced evolution of deepfake technology.

CONCLUSION:

Deepfake technology, leveraging artificial intelligence to create realistic fake videos, audio, and images, is becoming an increasingly potent tool for cybercriminals. In India, deepfakes are being used to commit various types of fraud, including identity theft, financial scams, and social engineering attacks. These activities pose serious risks to individuals, businesses, and government institutions, jeopardizing both personal privacy and the integrity of digital systems. The rise of deepfakes makes it easier for criminals to impersonate others and carry out fraudulent activities, such as stealing money or spreading misinformation. This is especially problematic for systems that rely on biometric identification methods, like facial recognition and voice authentication, as deepfakes can manipulate these technologies with alarming ease. Although Indian laws like the Information Technology Act, 2000 (IT Act) offer some protection by criminalizing identity theft and impersonation (under Sections 66C and 66D), they are not specifically designed to address the evolving nature of deepfake technology. The Indian Penal Code (IPC) also includes provisions for fraud and cheating, but these laws often fall short when dealing with the unique challenges posed by deepfakes.

BIBLIOGRAPHY:

1. Abdul-Rahman, Kabbara. “Bots & Deepfakes.” NSI Intern Integration Project, August 2021. https://nsiteam.com/social/wpcontent/uploads/2021/08/IIJO_eIntern-IP_Bots-and-Deepfakes_Kabbara_FINAL.pdf

2. Bharatiya Nyaya Sanhita, 2023, Law No. CG-DL-E-25122023-250883, Dec. 25, 2023. https://www.mha.gov.in/en/commoncontent/new-criminal-laws

3. Bhusal, Chandra Sekhar, Systematic Review on Social Engineering: Hacking by Manipulating Humans (2021). Journal of Information Security, 2021, 12, 104-114. Available at SSRN: https://ssrn.com/abstract=3821594

4. Benjamin Goggin, From Porn to ‘Game of Thrones’: How Deepfakes and Realistic-Looking Fake Videos Hit It Big, BUS. INSIDER (June 23, 2019, 10:45 AM). https://www.businessinsider.com/deepfakes-explained-the-rise-of-fake-realistic-videos-online-2019-6

5. Bureau (2024). Three Criminal Laws To Be Effective From July 1. The Hindu. [online] 24 Feb. https://www.thehindu.com/news/national/three-newly-enacted-criminal-laws-to-come-into-effect-from-july-1/article67881602.ece

6. Chesney, Bobby, and Danielle Citron. "Deep fakes: A looming challenge for privacy, democracy, and national security." Calif. L. Rev. vol.107 pp.1753. (2019)

7. Cruz-Neira, Carolina & Fernández, Marcos & Portalés, Cristina. ‘Virtual Reality and Games’. Multimodal Technologies and Interaction. vol. 2 pp. 8 (2018). DOI: https://doi.org/10.3390/mti2010008

8. Gilbert C. & Gilbert M.A. ‘The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges. Global Scientific Journals. ISSN-2320-9186, vol.12(9), pp.427-441. (2024). https://www.globalscientificjournal.com/researchpaper/

9. Gilbert, Chris & Gilbert, Mercy. ‘The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation’. International Research Journal of Advanced Engineering and Science, ISSN 2455-9024. pp.170-181. (2024)

10. Goh, D. H.-L., Lee, C. S., Chen, Z., Kuah, X. W., & Pang, Y. L. (2022). 'Understanding Users' Deepfake Video Verification Strategies. In C. Stephanidis, M. Antona, S. Ntoa, & G. Salvendy (Eds.), HCI International 2022 – Late Breaking Posters pp. 25–32. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-19682-9_4

11. Joseph Foley, 14 Deepfake Examples That Terrified and Amused the Internet, CREATIVE BLOQ (June 1, 2021). https://www.creativebloq.com/features/deepfake-examples

12. Karen Hao, Deepfake Porn is Ruining Women's Lives. Now the Law May Finally Ban It., MIT TECH. REV. (Feb. 12, 2021). https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-comingban/%20[https://perma.cc/PV9M-CKCH]

13. Koops, Bert-Jaap and Leenes, Ronald E. and Leenes, Ronald E., ID Theft, ID Fraud and/or ID-Related Crime - Definitions Matter. Datenschutz und Datensicherheit, Vol. 30, No. 9, pp. 553-556, 2006. Available at SSRN: https://ssrn.com/abstract=982076

14. Kristen Dold, Face-Swapping Porn: How a Creepy Internet Trend Could Threaten Democracy, ROLLING STONE (Apr. 17, 2018, 8:47 PM). https://www.rollingstone.com/culture/culture-features/face-swapping-porn-how-a-creepy-internet-trend-could-threaten-democracy-629275/

15. Mika Westerlund, 'The Emergence of Deepfake Technology: A Review', Technology Innovation Management Review, vol.9 no.11. Pp. 43. (2019)

16. Marissa Koopman, Andrea Macarulla Rodriguez, and Zeno Geradts. Detection of deepfake video manipulation. At the 20th Irish Machine Vision and Image Processing Conference (IMVIP), pages 133–136, 2018.

17. Ming-Yu Liu, Xun Huang, Jiahui Yu, Ting-Chun Wang, and Arun Mallya, 'Generative adversarial networks for image and video synthesis: Algorithms and applications. Proceedings of the IEEE, 109(5):839–862, 2021. https://arxiv.org/abs/2008.02793

18. Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. ACM Computing Surveys, 54(1), 7:1-7:41. https://doi.org/10.1145/3425780

19. Mullen, Molly 'A New Reality: Deepfake Technology and the World Around Us,' Mitchell Hamline Law Review: Vol. 48: Iss. 1, Article 5. (2022). Available at: https://open.mitchellhamline.edu/mhlr/vol48/iss1/5

20. Ndaba, Nomkhosi Lucia. "The impact of government employees using biometrics in IT security management at KZN Treasury." PhD diss., (2019). https://researchspace.ukzn.ac.za/server/api/core/bitstreams/932e900d-5444-4058-b2d3-3b23a6bd2198/content

21. Ruhl, Christopher A. "Corporate and Economic Espionage: A Model Penal Approach for Legal Deterrence to Theft of Corporate Trade Secrets and Proprietary Business Information." Valparaiso University Law Review vol.33, no. 2 763-811. (2011)

22. The Digital Personal Data Protection Act (DPDPA), 2023, No. 61 of 2023

23. The Indian Penal Code, 1860, Act No. 45 of 1860

24. The Information Technology Act, 2000, No. 21 of 2000

25. The Copyright Act, 1957, Act No. 14 of 1957

26. Vig, Shinu, 'Regulating Deepfakes: An Indian perspective'. Journal of Strategic Security vol. 17, no. 3 pp. 70-93. (2024). DOI: https://doi.org/10.5038/1944-0472.17.3.2245 Available at: https://digitalcommons.usf.edu/jss/vol17/iss3/5

27. Westerlund, Mika. The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review, 9(11), 40–53. (2019) https://doi.org/10.22215/timreview/1282

28. Karin Kelley, 'The Double-Edged Sword of AI Deepfakes: Implications and Innovations'. Centre for Technology and Management. https://pg-p.ctme.caltech.edu/blog/ai-ml/double-edged-sword-of-ai-deepfakes-implications-innovations

29. Mullen, Molly 'A New Reality: Deepfake Technology and the World Around Us' Mitchell Hamline Law Review: Vol. 48: Iss. 1, Article 5. (2022). Available at: https://open.mitchellhamline.edu/mhlr/vol48/iss1/5

30. T. T. Nguyen, C. M. Nguyen, D. T. Nguyen, D. T. Nguyen, and S. Nahavandi, "Deep Learning for Deepfakes Creation and Detection," arXiv preprint arXiv:1909.11573, 2019. https://arxiv.org/abs/1909.11573

31. Karin Kelley, 'The Double-Edged Sword of AI Deepfakes: Implications and Innovations'. Centre for Technology and Management. https://pg-p.ctme.caltech.edu/blog/ai-ml/double-edged-sword-of-ai-deepfakes-implications-innovations

32. Gilbert, Chris & Gilbert, Mercy. 'The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation'. International Research Journal of Advanced Engineering and Science, ISSN 2455-9024. pp.170-181. (2024)