Page 5838 - 5847

DOI: *https://doij.org/10.10000/IJLMH.1110254*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Emerging Dimensions of Criminality in the Age of Artificial Intelligence and Deepfakes: A Critical Study of Legal Remedies Available and Mitigation Strategies

PRASANNA KUMAR SHUKLA[1]

ABSTRACT

Rapid growth of technology like AI and deepfakes have significant impact on various sectors, however these have explored new dimensions of criminality in world with various challenges to legal and criminal justice created world of crime. It has AI and Deepfakes are causing rapid victimization of different groups of society.it is also hampering admissibility of evidences in court room, using these techniques photo, video, audio, document anything can be morphed. So apart from criminalization and victimization the process of justice delivery is getting hampered by AI and Deepfakes.it is challenge for individuals, state as well as world community. So in this paper the author has tried to find out different types of crime caused using AI and deepfakes, its impact and suggest legal, regulatory and policy framework for stopping criminality due to AI and Deepfake.

I. INTRODUCTION

In 21st century information technology and its uses are new parameters of development for any sector, for any country. Human is fully dependent on it for all kind of works.in information technology its most important part is Artificial intelligence. Not only dependency but faith of society is on AI. from automobiles to defense, study to jobs, court room to hospital everywhere one can see use of AI. it has made human life easier, better, saving time, energy and resources.

There is no precise definition of Artificial Intelligence.' In common parlance, it is "ability to adapt or improvise according to the feedback received in order to solve problems and address situations that go beyond the predefined set of queries and instructions that the AI was programmed with" (Padhy, 2019).

Artificial intelligence (AI) encompasses the advancement of computational systems capable of executing activities that conventionally need human intellect, including but not limited to visual perception, speech recognition, decision making, and language translation. (Dennis Trinkle,

[1] Author is a Guest Faculty at Government Law College, Indore, M.P., India.

2024). While deepfakes are a distinct use of artificial intelligence (AI) technology wherein digital photos and videos are manipulated to generate counterfeit material that closely resembles reality. The utilization of Deep Fakes encompasses a wide range of objectives, spanning from recreational amusement to the dissemination of political propaganda (Meenakshi Punia, 2024).

But like every coin has 2 sides AI have same. With rapid use of AI criminalization is increasing day by day. Deep fake content is very common, cyber-crimes, identity theft, privacy violations, different frauds, impersonation, ethical challenges,IPR Violations are very common types of crimes arising from Use of AI. While it is affecting the judicial system, decision making and hampering growth of criminal justice system. If talk about legal remedies available to overcome this criminalization due to AI no such strong legislation or guidelines are available in India. Although European union have its own kind of law to deal with such criminalization. AI and remedial measures to fight its ill effects have to developed together. Among various challenges of AI deciding criminal responsibility in act of criminalization is also a challenge.

II. Typology of criminalization due to artificial intelligence

Following are Various types of crimes arising due to AI.

1. Fraud

AI has increased and transformed types of fraudulent activities due to which it is difficult to detect these activities. From generating convincing phishing emails to creating deepfake voice and video content, AI-powered tools have expanded the arsenal of fraudsters, allowing them to target individuals and organizations with unprecedented precision and efficiency (LLP, 2023). Further fraud can be classified into various sub categories which are discussed below.

1.1 Executive Impersonation – AI and Deepfakes are used to impersonated reputed executives and Authorize fraudulent transactions.

1.2 Phishing email and bulk Messages- It is type of cyber attack where mails and messages are delivered with malicious links to steal personal information.

1.3 Spoofing- Here criminals uses important credentials like email, website, logo of renowned companies and persons to do financial scams.

1.4 Spear Phishing- Spear phishing is a targeted phishing attack on a user, usually via malicious emails. Spear phishing has proven to be the largest, most common, and most costly form of cyber threat, with an estimated 300,000 reported victims in 2021 representing $44 million in reported losses in the United States alone. (Batmaz, 2023)

1.5 Elder Fraud – AI is misused in these kind of frauds where emotional blackmailing of elders is done. Using deepfakes voice of there closed one such crimes are done.

1.6 Identity Fraud - Identity fraud has traditionally involved obtaining personal information to impersonate someone else, typically for financial gain.

1.7 Healthcare Fraud- AI can improve production that enables AI to learn and create medical records and imitate live voices, or de-anonymize data that can be used in fraud activities.

2. Market Manipulation –

Manipulation of share market is most common type of crime done using AI, where false apps are used. often it creating false or misleading appearances regarding the price or demand for securities market manipulation affects demand and supply chain of market. It is a growing concern for regulators and financial institutions.

3. Sextortion

It most common crime in era of AI. Kids, adults, elders all are prone to sextortion. It is a form of blackmail where perpetrators threaten to distribute explicit content unless the victim complies with their demands. Using deepfakes, criminal creates realistic videos and images showing indulgence in sexual activities. Even such sextortion causes incidents of suicide also.

4. Child sexual abuse Content-

In AI era child sexual abuse content is rapidly increased, normal images and videos are converted in pornography material by offender, adult pornography is also modified into child pornography. Animation content is also generated.

5. Misinformation and Propaganda

This is biggest area which is affected by Using AI to spread false news, for political manipulation and running paid agenda of particular groups. Recently such deepfakes video was reason of big riot in India and last 2 US presidential elections were also affected by it. (How AI Is Being Abused to Create Child Sexual Abuse Imagery, 2023)

6. National Security Threats

AI in place of Honest, helpful, harmless is proving reason for violent crimes, Terrorism and radicalization. Using AI Drone attacks,cyber terrorism is most common. Using AI cyber physical attacks are also done at national information centers.

7. Data Privacy Breaches

AI has revolutionized data processing and analytics, offering unprecedented capabilities in various sectors. However, this technological advancement comes with significant privacy risks, particularly concerning unauthorized data access and breaches. As AI systems increasingly rely on vast amounts of sensitive data to function effectively, they become prime targets for exploitation and cyberattack. Cybercriminals can target AI systems to exploit vulnerabilities and gain unauthorized access to sensitive information, such as personal data, financial records, or research data. The extensive use of AI in processing large data sets makes these systems particularly attractive to hackers. (AI and Privacy: The Privacy Concerns Surrounding AI, Its Potential Impact on Personal Data.", 2023)

8. Economic Crimes-

Various economic crimes such as corporate espionage,market manipulation is done using AI.

9. Intellectual Property Rights Violation

Violation of IPR is also Crime, Violation of IPR Law is most Common happening in Cyber world.

III. Challenges

As discussed above different type of crimes around the world due to rapid growth of AI and Deepfake. This robust criminalization is raising new challenges

1. Legal Challenges – Crimes due to AI and Deepfake are becoming transnational, due to lack of regulatory measure and law offenders are roaming freely in nation as well as outside of Nation. It is also creating impact on legal and decision-making of judicial system. AI ability to create deceptive depictions challenges the authenticity of AI systems used in the legal profession. (C. F. Kerry, 2021) It is also used to tempering evidence and hamper process of Judiciary.
2. Ethical Challenges- Misinformation and privacy violation is disrupting trust of society. Responsibility,accountability and transparency of Technology is in question.
3. Social Challenges- Due to interruption of AI society is dividing which is major challenges for unity and integrity of nation.
4. Technical Challenges – Due to misuse of AI its biggest challenge for world IT Industry to keep away this from offender and crimes and protect human rights.

IV. Liability of AI born crimes

It’s an easy task to control any crime and stop criminalization if you know of offenders and liable person or corporation. but what if its not known. AI and Deepfakes world crime are creating similar challenges to our criminal justice system. One can consider AI as separate entity but what will be the extent of liability, who will be liable for Such act is still in question. The following are possible options for deciding criminal Liability of AI entities.

1. When AI is acting as an innocent agent- AI entity is presumed to be an innocent agent working according to the instructions of the user. In such a case, criminal liability can arise because of intentional programming by the producer to commit an offence, or misuse of the AI entity by the user for commission of the crime? (Padhy, 2019) So its tuff task to decide whether producer, end user and intermediary is liable.
2. When Al is acting as semi-innocent agent - possible situation is based on the foreseeability of the producer/programmer or end user as to the potential commission of offences. In this particular situation, the producer and the user work closely with the AI entity though they did not intend the particular offence. In such a case, criminal liability can arise in two ways- First, because of negligence or recklessness of the producer in programming the AI entity and second, natural and probable consequence of the act instructed by the user (Padhy, 2019).
3. When Al is acting an independent entity/fully autonomous - In future, AI entities may be able to function in a totally independent, fully autonomous manner, not solely dependent on the algorithms rather than learning from their experiences and observations. Such AI entity would have the cognitive capabilities i.e. the ability to choose between alternate possible solutions to a problem. If such AI entity commits a crime, then such AI entity can be held criminally liable (Padhy, 2019).

Other such challenge is what will be the defences for such liability and what will be the punishment if found guilty of crime.

V. Legal remedies

Till now very few efforts have been done to deal with criminality arising due AI and Deepfakes in Indian as well as Global Context. These efforts are complex and far reaching

In India Perspective – India have its Own IT Act with deals with certain kind of crimes. India's Personal Data Protection Bill addresses data privacy issues, and other IT laws may apply to AI and deep fakes. although it lacks liability and accountability part of offences occurred using AI and deepfakes. Apart from IT act Indian Constitution Also Protects Privacy. IF infringement of IPR is done then it will be governed using related IPR Law. Defamation laws also applied when it is done using AI and Deepfakes. Deceptive Deepfakes also covered Under BNS.Overall we can say that India needs sector Specific rules Related to Crimes caused using AI and Deepfakes. although Despite lacking a specific framework, existing rules can address deepfake issues.

In Global Perspective – GDPR guide data protection in AI Regime, various countries have sector specific rules to deal with AI. For IPR violation local IPR laws are applied.

1. Council of Europe - Recommendations on ethical and legal aspects of AI Is Given but No specific legal framework for AI and deepfakes (Meenakshi Punia, 2024).
2. European Union (EU) - GDPR offers some protections against the misuse of personal data in AI and deepfake contexts. Further Developing a comprehensive AI legal framework (Jadhav, 2023).
3. United States- No federal AI and deepfake law; existing laws cover IP, privacy, consumer protection, with First Amendment considerations (Edwards, 2021). The Deepfake Accountability Act (Ice, 2019) aims to hold creators, distributors, and consumers accountable with labeling, reporting, and usage restrictions.
4. Asia - AI regulations vary across Asian nations. China has sector specific AI regulations in healthcare, finance, and education. Lack of specific deepfake framework.

Mitigation strategies

Identifying, addressing, and prosecuting the deepfake threat, especially when propagated by domestic extremists, will be no small feat for law enforcement. effective mitigation of threats from AI-related crime requires a range of complementary efforts broadly comprising improved collaboration and information-sharing, more training and awareness efforts aimed at the public, harnessing AI to combat AI threats, and borrowing well-developed strategies from the cybersecurity sector (Ware, 2023). Such mitigation strategies can be used to combat rising criminality due to AI And Deepfakes.

1. Legal and Policy measure – Amend existing law and make new laws to deal with AI driven crimes. Decide accountability and liability of users and producers of program if found guilty. Strict sentence and penalty should be used.
2. Technical Advancement - Use blockchain to track Origin of AI driven offences or cause of criminality. Develop new tools to detect AI driven crime. Advancement of AI Forensics should be done.

3. International Corporation- to tackle criminality arising from AI transnational laws need to be made. Cooperation and coordination must be there. UN level watchdog must be there to deal with Criminality arose due to AI. Cross border framework must be there.
4. Education and awareness- cyber hygiene must be part of day to day life of Netizens of cyber world.

VI. Conclusion

In Era of Artificial Intelligence rapid growth of different type of crimes is raising question on safety of users and world community. Day by day new type of threats can be seen AI World. in one hand it is making life of people easy, comfortable saving time and energy on other hand its throwing them into hands of offender. To deal with such crime is accountability and liability. To deal with any criminal act you to fix Liability and accountability then proper penalty and punishment can be imposed. In AI driven crimes it impossible to fix liability. First its need of hour to work on liability then control on offenders can be done. In India level no specific law available to deal with AI driven offences. Some offences are covered in specific laws like IPR, Defamation law, IT Law, BNS etc. so there is need of dedicated law. While if talk about world level sectors specific laws are present to deal with AI driven Crimes. Its urgent need of hour to develop legislation at internation and national level to deal with Rising criminality due to AI and deepfake to world community. This study can be said as urgent need to understand the challenges given by AI and deepfakes in criminal justice system. It can be done by exploring different aspects of legal, cyber, technological, societal, policy and governance related aspects. It is important for protecting individuals, society from criminalization and victimization, gaining there trust in technologies and providing them benefit of such technologies.

VII. References

1. (n.d.). Retrieved from file:///G:/phd/AI%20and%20deep%20fake/5a265f6b-be02-4f18-9d1e-86b55d0bc1b4.pdf
2. AI and Privacy: The Privacy Concerns Surrounding AI, Its Potential Impact on Personal Data.". (2023).
3. Batmaz, S. D. (2023, September 12). Generative AI and Accelerated Computing for Spear Phishing Detection.". *NVIDIA Technical Blog*.
4. C. F. Kerry, J. P. (2021). Strengthening international cooperation on AI. Retrieved from https://www.brookings.edu/articles/strengthening-international-cooperation-on-ai/
5. Dennis Trinkle, H. M. (2024, June). Artificial Intelligence and the Indiana workforce-A Swift and pervasive transformation. Retrieved from https://techpoint.org/artificial-intelligence/
6. Edwards, L. (2021). Expert explainer: The EU AI Act proposal. *Adalovelaceinstitute.org*.
7. (2023, October). *How AI Is Being Abused to Create Child Sexual Abuse Imagery.* Internet watch Foundation.
8. Ice, J. (2019). Defamatory Political Deepfakes and the First Amendment. *Case Western Reserve Law Review 2019*.
9. Jadhav, S. P. (2023). Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India. *SCC Online*.
10. LLP, P. (2023). *Impact of Artificial Intelligence on Fraud and Scams.*
11. Meenakshi Punia, A. G. (2024, September 30). Deepfakes,Deception and The Law-Unraveling the Legal Complexities of AI-Generated Content. *Springer Nature*. doi:https://doi.org/10.1007/978-981-97-3690-4_56
12. 'भारत में अपराध | National Crime Records Bureau' (*ncrb.gov.in*) <https://ncrb.gov.in/crime-in-india.html>
13. Busch E and Ware J, 'The Weaponization of Deepfakes Digital Deception by the Far-Right' (2023) <https://www.icct.nl/sites/default/files/2023-12/The%20Weaponisation%20of%20Deepfakes.pdf>

14. Department of Homeland Security, 'Increasing Threat of Deepfake Identities' (2023) <https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf>

15. Felipe Romero Moreno, 'Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content' [2024] International review of law computers & technology 1

16. Hailtik AGE and Afifah W, 'Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia' (2023) 2 Asian Journal of Social and Humanities 776 <http://www.ajosh.org/index.php/jsh/article/view/222> accessed 22 February 2024

17. ——, 'Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia' (2023) 2 Asian Journal of Social and Humanities 776 <http://www.ajosh.org/index.php/jsh/article/view/222>

18. Mateusz Łabuz, 'Regulating Deep Fakes in the Artificial Intelligence Act' (2023) 2 Applied Cybersecurity & Internet Governance

19. 'MeitY Issues Advisory to All Intermediaries to Comply with Existing IT Rules.' (*pib.gov.in*) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542>

20. Muaath S and Al-Mulla, 'Deepfakes: Criminalization and Legalization Analytical Descriptive Study Associate Professor of Criminal Law -Faculty Member at Kuwait International Law School, State of Kuwait' (2022) 19 3210 <https://www.webology.org/data-cms/articles/20220219124153pmwebology%2019%20(2)%20-%20238%20pdf.pdf> accessed 15 July 2024

21. 'Publication | Does the UN Need a Watchdog to Fight Deepfakes and Other AI Threats?' (*www.gcsp.ch*) <https://www.gcsp.ch/publications/does-un-need-watchdog-fight-deepfakes-and-other-ai-threats> accessed 15 July 2024

22. 'The 2021 Innovations Dialogue: Deepfakes, Trust and International Security → UNIDIR' (*unidir.org*25 August 2021) <https://unidir.org/event/the-2021-innovations-dialogue-deepfakes-trust-and-international-security/>

23. Zubair A, Khan and Rizvi M, 'Deepfakes: A Challenge for Women Security and Privacy' <https://www.cmr.edu.in/school-of-legal-studies/journal/wp-

content/uploads/2024/01/Deepfakes-A-Challenge-for-Women-Security-and-Privacy-Dr.-Zubair-Ahmed-Khan-_-Ms.-Asma-Rizvi.pdf> accessed 4 June 2024

24. Padhy, A. K. (2019). CRIMINAL LIABILITY OF. *Nirma University Law Journal:, 8*(02), 15-20.

25. Ware, E. B. (2023). The Weaponisation of Deepfakes Digital Deception by the Far-Right. *ICCT Policy Brief*. Retrieved from https://icct.nl/sites/default/files/2023-12/The%20Weaponisation%20of%20Deepfakes.pdf

*****