



Digital Evidence and Deepfake: A Challenge to Criminal Justice System in India

¹Dr. Ajit Singh, Ph.D. (Law) Registrar, Capital University, Jharkhand

²Dr. Pawan Kumar, Ph.D. (Law) Chancellor, Mahatma Gandhi University, Sikkim

Corresponding Author: Chaudharyajit29@gmail.com

Abstract: In the digital age, the emergence of deepfake technology has posed unprecedented challenges to legal systems worldwide, particularly in the realm of digital evidence. This paper explores the implications of deepfake videos and AI-generated content on India's criminal justice system. It evaluates the adequacy of existing legal frameworks, judicial preparedness, and the technological challenges of identifying manipulated digital media. The study proposes reforms to ensure the authenticity, admissibility, and ethical handling of digital evidence, safeguarding justice in an era of artificial manipulation.

Keywords: Criminal Justice System, Deepfake technology, AI-generated content, Digital Evidence

1. Introduction

The incorporation of digital evidence in the Indian judicial process has become increasingly common. Videos, audios, and digital documents now play a crucial role in criminal trials. However, the rise of deepfake technology AI-driven media manipulation that can fabricate hyper-realistic content raises concerns about the credibility of such evidence. This paper examines the legal, technological, and ethical dimensions of deepfakes and their potential to disrupt justice delivery.

2. Understanding Deepfake Technology

Deepfakes are synthetic media in which a person's likeness is replaced with someone else's using artificial intelligence, particularly Generative Adversarial Networks (GANs). Initially developed for entertainment, deepfakes now serve malicious purposes including political misinformation, character assassination, and criminal fraud. The ease of access to deepfake tools makes this threat accessible to the masses.

Technically, deepfakes are created using large datasets of images and voice samples, enabling machine learning models to accurately mimic expressions, voice patterns, and gestures. As this technology becomes more refined and accessible, it increases the potential misuse in areas like pornography, election manipulation, and courtroom evidence.

3. Legal Framework Governing Digital Evidence in India

India's legal framework for digital evidence includes:

- The Indian Evidence Act, 1872: Sections 65A and 65B address the admissibility of electronic records, requiring a certificate for authenticity under Section 65B(4).
- The Information Technology Act, 2000: Addresses cybercrime and data protection but lacks specificity regarding AI-generated content and manipulated media.

- Indian Penal Code (IPC): Sections on forgery (Section 465), defamation (Section 499), obscenity (Section 292), and cyberstalking (Section 354D) can apply to deepfake misuse.

However, there is no explicit legal recognition of deepfake content as a separate offence. Further, the procedural hurdles in admitting digital evidence, such as obtaining Section 65B certificates, often weaken the prosecution.

4. Global Perspectives

Countries like the USA and the UK have begun enacting laws to combat deepfakes. In 2019, the US passed the DEEPFAKES Accountability Act, criminalizing malicious deepfake creation. California has passed laws banning political deepfakes within 60 days of an election. In the UK, deepfakes are tackled under harassment, fraud, copyright infringement, and the Online Safety Bill.

China has introduced regulations requiring deepfake content to be clearly marked, and South Korea criminalizes the production and distribution of sexual deepfakes. These proactive measures highlight the urgency of a similar approach in India.

5. Literature Review

Recent academic literature highlights deepfakes as a growing global concern. Scholars argue for new jurisprudence that integrates AI ethics, forensic science, and legal reform. A 2023 study by the International Journal of Cyber Law concludes that over 70% of surveyed legal professionals found current digital evidence laws insufficient to handle AI-generated content. Another report by NITI Aayog emphasizes the need for ethical AI use in governance and judiciary. The lack of case law and the novelty of the issue make scholarly recommendations vital in shaping the legal discourse.

6. Challenges for Indian Judiciary and Law Enforcement

- Authentication Difficulties: Deepfakes are often indistinguishable from real media without advanced forensic tools, leading to potential miscarriages of justice.
- Lack of Expertise: Judges and lawyers may lack technical training to identify or interpret deepfakes, especially in lower courts.
- Forensic Limitations: India lacks standardized deepfake detection tools and qualified forensic experts.
- Delay in Legal Reform: The legislature has yet to respond adequately to the rapid advancements in AI technology.
- Jurisdictional Complexity: Content created outside India but impacting Indian citizens poses jurisdictional enforcement challenges.

7. Judicial Trends and Case Studies

Although deepfake-related cases in India are still emerging, notable incidents include:

- Misuse of morphed videos during state and general elections.
- Circulation of fake pornographic content using public figures' images on social media platforms.
- A 2022 Delhi court case involved a deepfake used to manipulate surveillance footage in a theft trial, raising concerns over chain of custody and digital manipulation.

These instances underline the urgent need for judicial cognizance and proactive rulings. In landmark judgment *Anvar P.V. v. P.K. Basheer* (2014), the Supreme Court stressed the importance of Section 65B compliance for electronic evidence. However, the ruling also highlighted procedural rigidity that could be exploited in the age of deepfakes.

8. Recommendations and Reforms

- Legislative Reform: Enactment of a dedicated "Deepfake Regulation Act" which criminalizes malicious creation and distribution of deepfakes.
- Capacity Building: Mandatory training for police, prosecutors, and judges on AI, forensic validation, and cyberlaw.
- Technological Collaboration: Encourage partnerships between legal institutions and tech companies to develop deepfake detection tools.
- Public Awareness Campaigns: Run national-level awareness drives to educate citizens about the existence and dangers of deepfakes.
- Digital Evidence Certification Authority: Establish a national authority under the Ministry of Law or Ministry of Electronics & IT to certify the authenticity of digital submissions.
- Fast-Track Courts for Cybercrimes: Establish specialized courts to handle digital evidence disputes promptly.

9. Conclusion

Deepfakes represent a significant threat to the integrity of India's criminal justice system. As technology evolves, so must the law. The Indian judiciary and legislature must act swiftly to address this growing menace. Only through legal reform, technological advancement, and institutional awareness can justice be preserved in a digitally manipulated world.

The window of opportunity to act is narrow. India must proactively equip its legal ecosystem to respond to this AI-driven crisis, or risk seeing the foundation of justice shaken by synthetic lies.

References

1. Indian Evidence Act, 1872
2. Information Technology Act, 2000
3. IPC Sections 465, 499, 292, 354D
4. DEEPFAKES Accountability Act, USA (2019)
5. California Political Cybercrime Law (2020)
6. Supreme Court judgment: Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
7. International Journal of Cyber Criminology, Vol. 17, 2023
8. NITI Aayog Report on Responsible AI, 2021
9. OECD AI Policy Framework, 2022
10. Ministry of Electronics & IT, Deepfake Awareness Report, 2023
11. UK Online Safety Bill, 2023
12. South Korea AI Abuse Law, 2022