International Journal of Business Management and Legal Affairs ijbmla.com
ISSN: 3107-8648
Volume 1: Issue 3, Jul-Sep 2025 Open Access

DEEPFAKE TECHNOLOGY AS AN EMERGING TOOL OF CYBERCRIME: LEGAL CHALLENGES AND REGULATORY RESPONSES IN INDIA

Dr. R. N. Mangoli[1], Dr. Rajratna Jadhav[2]
[1]Professor, Dept. of Criminology and Forensic Science, Rani Channamma Univesity, Belagavi, Karnataka, India. Email - drmangoli.rn@rcub.ac.in

[2]Research Associate, Maharashtra National Law University Mumbai, Powai, Mumbai, Maharashtra, India. Email - rajadhv7@gmail.com

ABSTRACT

The rapid advancement of artificial intelligence has significantly transformed the digital environment, enabling the creation of highly realistic synthetic media commonly known as deepfakes. While deepfake technology offers several beneficial applications in entertainment, media production, and digital communication, it has increasingly emerged as a powerful tool for cybercrime. The misuse of deepfake technology has facilitated various forms of online offences. As these technologies become more accessible, the potential for their misuse poses serious challenges to cybersecurity, privacy, and digital trust.

This research article examines deepfake technology as an emerging instrument of cybercrime within the Indian legal context. The study adopts a doctrinal research methodology based on the analysis of statutes, judicial decisions, academic literature, and policy reports relating to cyber law and artificial intelligence. It critically evaluates the applicability of existing legal provisions, including those under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 in addressing deepfake-related offences.

The article further explores recent judicial developments concerning digital impersonation and personality rights, highlighting how courts are increasingly confronted with disputes involving synthetic media. The study argues that although existing legal provisions offer partial remedies, they are insufficient to effectively address the complex challenges posed by deepfake-enabled cybercrime. The paper concludes by recommending the development of clearer regulatory frameworks, enhanced platform accountability, and greater investment in technological detection mechanisms to combat the misuse of deepfake technology in India.

Keywords *Deepfake technology, Cybercrime, Artificial Intelligence, Digital Impersonation, Cyber Law, Cybersecurity.*

1. INTRODUCTION

The expansion of digital technologies and artificial intelligence has significantly transformed the manner in which information is created, shared, and consumed in modern society. Among the most controversial innovations in recent years is deepfake technology, which allows the creation of highly realistic synthetic media using artificial intelligence and machine learning techniques. Deepfakes involve the manipulation of images, audio recordings, or videos in such a way that they appear authentic despite being entirely fabricated.

Deepfakes involve the manipulation of audio, images, or video content using artificial intelligence techniques such as deep learning and generative adversarial networks (GANs). These technologies enable the creation of fabricated media that appears authentic and can convincingly replicate the appearance or voice of real individuals. While the technology has

legitimate uses in film production, digital art, and educational simulations, its misuse has raised serious concerns regarding cybercrime and digital misinformation.

The proliferation of deepfake technology has significant implications for cybersecurity and the protection of individual rights. The increasing accessibility of AI-based tools means that individuals with minimal technical expertise can generate manipulated digital content capable of misleading audiences. As a result, deepfakes have become a powerful instrument for fraud, defamation, identity theft, and online harassment.

Recent incidents demonstrate the growing risks associated with deepfake technology. For instance, cybercriminals recently defrauded a student in Bengaluru of approximately ₹3.5 lakh by using a deepfake video impersonating a government official to promote a fraudulent investment scheme.

Similarly, another case involved a farmer in Uttarakhand who was deceived through a deepfake voice call mimicking his son and subsequently transferred ₹6 lakh to fraudsters.

These incidents illustrate how deepfake technology can be exploited to manipulate victims and facilitate financial fraud.

In India, the growing digital population and widespread use of social media platforms have created an environment in which manipulated digital content can rapidly spread across networks. However, the legal framework governing cybercrime has not evolved at the same pace as technological developments. Scholars have observed that existing laws such as the Information Technology Act, 2000 and traditional criminal statutes were not designed to address crimes involving advanced artificial intelligence technologies.

Therefore, it is essential to critically examine whether the current legal framework is capable of addressing the emerging threat posed by deepfake technology.

2. RESEARCH OBJECTIVES

- To evaluate the adequacy of the existing legal framework in India.
- To examine the challenges in regulating deepfake technology
- To propose policy measures to address deepfake-enabled cybercrime.

3. RESEARCH METHODOLOGY

This research adopts a doctrinal legal research methodology. The study relies on secondary sources including statutes, judicial decisions, government reports, academic literature, and policy documents relating to cyber law and artificial intelligence.

The analysis focuses on the applicability of existing legal provisions under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 to deepfake-related offences. Judicial decisions involving personality rights and digital impersonation have also been examined to understand how courts are addressing emerging challenges associated with synthetic media.

4. TECHNOLOGY AND FUNCTIONING OF DEEPFAKES

Deepfake technology is primarily based on artificial intelligence techniques known as deep learning. These systems rely on neural networks capable of analysing vast amounts of data in order to generate realistic synthetic media.

The most common technique used in deepfake creation is the generative adversarial network (GAN). GANs involve two neural networks that compete with each other: one generates synthetic content while the other attempts to detect whether the content is genuine or artificial. Through repeated iterations, the system gradually improves its ability to produce highly convincing manipulated media.

Although deepfake technology can be used for legitimate purposes, such as film production or language translation, its misuse has significant social and legal implications. Manipulated videos and audio recordings can easily mislead audiences, creating opportunities for fraud and misinformation.

5. DEEPFAKES AS A TOOL OF CYBERCRIME

Deepfake technology has increasingly been used as a tool for cybercrime.

- Identity Theft
  Deepfakes can replicate an individual's face or voice to impersonate them in digital communications. Such impersonation can be used to deceive victims or obtain confidential information.
- Financial Fraud
  Deepfake videos or audio recordings can be used to impersonate corporate executives, government officials, or financial advisors in order to deceive individuals into transferring money.
- Non-consensual Explicit Content
  One of the most harmful uses of deepfake technology involves the creation of non-consensual intimate images. Such content can severely harm victims' dignity and reputation. Recent reports have highlighted how AI-generated explicit images and "nudifying" applications are increasingly used to harass women online.
- Political Misinformation
  Deepfakes can also be used to manipulate public opinion by fabricating speeches or statements attributed to political leaders.

6. LEGAL FRAMEWORK GOVERNING DEEPFAKES IN INDIA

India presently lacks a dedicated legislation specifically regulating deepfake technology. Consequently, offences arising from the creation and dissemination of deepfakes are addressed through a combination of provisions contained in the Information Technology Act, 2000 (IT Act), the Bharatiya Nyaya Sanhita, 2023 (BNS), the Digital Personal Data Protection Act, 2023 (DPDP Act), and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Although these statutes were not enacted specifically to address artificial intelligence-generated content, they provide a legal basis for prosecuting various forms of deepfake-enabled cybercrime.

- **Information Technology Act, 2000**

  The IT Act remains the principal legislation governing cyber offences in India. Several provisions of the Act may be invoked depending upon the nature of the deepfake offence.

  Section 66C (Identity Theft) becomes relevant when an individual's image, voice, biometric features, or digital identity is used without authorization to create deceptive AI-generated content.

Section 66D (Cheating by Personation) is particularly important in cases involving deepfake-enabled fraud. AI-generated videos and voice clones are increasingly used to impersonate public officials, corporate executives, celebrities, or family members in order to deceive victims and obtain money or sensitive information.

Section 66E (Violation of Privacy) may be invoked where deepfake technology is used to create or circulate manipulated intimate content without the consent of the individual concerned.

Further, **Sections 67, 67A, and 67B** deal with the publication and transmission of obscene, sexually explicit, and child sexual abuse material in electronic form. These provisions are especially relevant in addressing non-consensual sexual deepfakes, which constitute one of the most prevalent forms of deepfake abuse globally.

- **Bharatiya Nyaya Sanhita, 2023**

  The Bharatiya Nyaya Sanhita, 2023 does not expressly define or criminalise deepfakes. However, several provisions may be applied depending upon the harm caused by synthetic media. Scholars have noted that deepfake offences often fall within existing categories such as forgery, defamation, impersonation, misinformation, and intimidation.

  Section 336 (Forgery) is one of the most relevant provisions. A malicious deepfake essentially creates a false electronic representation intended to deceive viewers. Where such fabricated content is used to cause injury, damage reputation, or obtain wrongful gain, liability for forgery may arise.

  Section 351 (Criminal Intimidation) may apply where fabricated videos or images are used to threaten, blackmail, or extort victims. This is particularly relevant in cases of deepfake-enabled sextortion and online harassment.

  Section 353 (Statements Conducing to Public Mischief) assumes significance in cases involving misinformation and disinformation. Deepfake videos capable of creating panic, disturbing public order, inciting communal tensions, or spreading false narratives may attract liability under this provision.

  Section 356 (Defamation) can be invoked where deepfake content harms an individual's reputation by falsely depicting them engaging in criminal, immoral, or objectionable conduct.

- **Digital Personal Data Protection Act, 2023**

  The creation of deepfakes frequently involves the collection and processing of personal data such as photographs, videos, voice samples, and biometric information. The DPDP Act, 2023 emphasises lawful processing of personal data based on consent and reasonable safeguards. Therefore, the unauthorized use of personal information for generating deepfake content may constitute a violation of data protection principles and attract regulatory consequences.

While the combined application of the IT Act, the BNS, and the DPDP Act provides certain remedies against deepfake-related harms, the existing framework remains fragmented. None of these statutes specifically define deepfakes or prescribe dedicated penalties for their malicious creation and dissemination. As a result, investigators and courts are often compelled to fit deepfake-related conduct into traditional legal categories such as forgery, defamation,

cheating, obscenity, and identity theft. This legislative gap has prompted increasing calls for a comprehensive legal framework specifically addressing artificial intelligence-generated synthetic media in India.

7. JUDICIAL RESPONSES TO DEEPFAKE MISUSE

Although India does not yet have a dedicated statute regulating deepfake technology, Indian courts have increasingly relied upon the doctrines of personality rights, privacy, publicity rights, and reputation to address the misuse of artificial intelligence-generated content. Recent judicial interventions indicate that courts are willing to extend existing legal principles to protect individuals from digital impersonation and synthetic media abuse.

- **Anil Kapoor v. Simply Life India & Ors. (2023)**

  One of the most significant Indian decisions concerning AI-generated content is *Anil Kapoor v. Simply Life India & Ors.* decided by the Delhi High Court in 2023. The plaintiff sought protection against the unauthorised use of his name, image, voice, likeness, and the well-known expression "Jhakaas" through various online platforms and AI-generated content.

  The Court recognised that technological developments, including artificial intelligence and deepfake technology, have created new threats to personality rights. It observed that the unauthorised use of a person's identity through manipulated digital content may cause reputational harm and violate the individual's right to dignity and privacy. Accordingly, the Delhi High Court granted an ex parte injunction restraining the defendants from using Anil Kapoor's name, voice, image, likeness, mannerisms, and other personality attributes without authorisation. The Court also directed the removal of infringing content from online platforms.

  The significance of this decision lies in its recognition that personality rights extend to protection against AI-generated deepfakes and digital impersonation. It remains one of the most frequently cited Indian cases concerning the misuse of artificial intelligence in relation to individual identity and reputation.

- **Rajat Sharma v. Google LLC & Ors. (2024–2025)**

  A more direct judicial response to deepfake technology can be seen in proceedings initiated by senior journalist Rajat Sharma before the Delhi High Court. Sharma approached the Court alleging that fabricated and deepfake videos using his likeness were being circulated on digital platforms.

  The Delhi High Court directed Google and YouTube to remove channels hosting deepfake videos and further ordered disclosure of information relating to the creators of such content. The Court recognised that deepfake videos have the potential to mislead the public, damage reputation, and undermine trust in digital information.

- **Public Interest Litigation on Deepfake Regulation**

  Recognising the broader societal threat posed by synthetic media, the Delhi High Court has also sought responses from the Central Government regarding measures adopted to address deepfake technology. During proceedings relating to deepfake regulation, the Court observed that the increasing misuse of AI-generated content presents serious concerns for privacy, public trust, and digital safety.

The Court directed the Government to submit a status report outlining steps taken to combat deepfake-related harms. Although the proceedings have not yet resulted in a comprehensive judicial framework, they reflect growing judicial concern regarding the absence of specific legislation addressing artificial intelligence-generated misinformation and impersonation.

The above decisions reveal a clear trend in Indian jurisprudence. Courts have increasingly relied upon personality rights, privacy rights, and the right to dignity under Article 21 of the Constitution to address harms caused by synthetic media. However, these decisions also highlight the limitations of the current legal framework. Most cases have been decided through the application of existing principles relating to identity, reputation, and publicity rights rather than through a dedicated statutory regime governing deepfakes.

8. COMPARATIVE REGULATORY APPROACHES TO DEEPFAKE GOVERNANCE

The European Union has emerged as one of the leading jurisdictions in regulating artificial intelligence and synthetic media through its risk-based regulatory framework. The recently adopted AI Act introduces transparency obligations for AI systems that generate or manipulate audio, video, and image content. Providers and deployers of such systems are required to disclose when content has been artificially generated or significantly altered, thereby enabling users to distinguish authentic content from synthetic media. In addition, the Digital Services Act places responsibility on large online platforms to mitigate risks arising from misinformation and manipulated content. Rather than imposing a blanket prohibition on deepfakes, the European approach focuses on transparency, accountability, and informed user choice while simultaneously protecting innovation and freedom of expression.

China has adopted a significantly stricter and more interventionist model of regulation. Through its Deep Synthesis Provisions and subsequent AI-content labelling regulations, China requires synthetic media providers to clearly label AI-generated content, verify user identities, obtain consent for the creation of deepfakes involving real persons, and maintain mechanisms that ensure traceability of manipulated content. The Chinese framework also prohibits the use of deepfake technology in ways that may threaten national security, public order, or social stability. Unlike the European Union, which primarily relies upon transparency obligations, China emphasises preventive regulation, platform responsibility, and strong governmental oversight. This approach reflects China's broader philosophy of digital governance, where technological innovation is permitted but remains subject to extensive regulatory supervision.

The United States follows a comparatively fragmented regulatory model. Instead of a comprehensive federal deepfake law, regulation has largely developed through state legislation, civil remedies, and sector-specific interventions. Various states have enacted laws targeting election-related deepfakes, non-consensual intimate imagery, and digital impersonation, while recent federal initiatives such as the TAKE IT DOWN Act seek to provide stronger protection against AI-generated sexual content and harmful impersonations. Consequently, the American approach relies heavily on privacy rights, publicity rights, intellectual property doctrines, and litigation-based remedies rather than a unified statutory framework. A comparative assessment of these jurisdictions suggests that India may benefit from adopting a balanced approach that combines the European emphasis on transparency, the Chinese focus on traceability and platform accountability, and the American recognition of individual rights and legal remedies. Such a hybrid framework could provide a more comprehensive response to the growing challenges posed by deepfake-enabled cybercrime.

9. CHALLENGES IN REGULATING DEEPFAKE TECHNOLOGY

Despite the growing recognition of deepfake-enabled cybercrime, regulating this emerging technology presents several complex legal, technological, and institutional challenges. The rapid evolution of artificial intelligence tools has significantly outpaced the development of legal frameworks, making it difficult for regulatory authorities to effectively control the misuse of synthetic media.

- **Difficulty in Detecting Deepfakes**

  One of the most significant challenges in regulating deepfakes lies in the difficulty of accurately detecting manipulated media. Advances in artificial intelligence have made it possible to generate highly realistic audio and video content that is often indistinguishable from genuine recordings. Research indicates that human observers are often unable to reliably distinguish deepfake videos from authentic ones. In fact, studies suggest that individuals correctly identify high-quality deepfakes only about 24.5% of the time, demonstrating the effectiveness of modern AI-generated manipulation techniques. Also, deepfake detection algorithms themselves face technical limitations. Detection models frequently rely on known datasets and may fail when confronted with new or previously unseen manipulation techniques.

  These limitations significantly complicate the work of law-enforcement agencies and digital forensic investigators.

- **Rapid Technological Advancement**

  Artificial intelligence technology is evolving at an unprecedented pace. Tools capable of generating convincing deepfake videos or voice clones are becoming increasingly accessible to the general public. Recent reports indicate that deepfake fraud has increased dramatically in recent years, with some regions experiencing increases exceeding 1500% in deepfake-related fraud incidents. Because new AI models are constantly being developed, legal regulations often become outdated shortly after they are introduced.

- **Cross-Border Jurisdictional Challenges**

  Cybercrime frequently transcends national borders, and deepfake misuse is no exception. Manipulated media may be created in one jurisdiction, hosted on servers located in another country, and circulated globally through social media platforms. This transnational nature of cybercrime creates serious enforcement challenges for national legal systems. Law-enforcement agencies often face difficulties in identifying perpetrators, obtaining digital evidence, and coordinating international investigations.

- **Inadequate Legal Frameworks**

  Another major challenge is the absence of specific legislation addressing deepfake technology in many jurisdictions. Existing laws governing cybercrime, privacy, defamation, and fraud were generally enacted before the emergence of artificial intelligence-generated synthetic media. Consequently, courts often rely on traditional legal doctrines such as impersonation, defamation, or identity theft to address deepfake-related disputes. While these provisions provide partial remedies, they do not fully capture the unique characteristics of deepfake manipulation.

Researchers have noted that deepfakes can threaten privacy, reputation, and even national security by facilitating misinformation and electoral manipulation.

- **Social Media Amplification**

  Digital platforms play a critical role in the rapid dissemination of deepfake content. Social media algorithms often prioritize engaging content, which may inadvertently amplify manipulated videos and sensational misinformation. Once such content goes viral, it becomes extremely difficult to remove or correct the misinformation. Even if the original content is deleted, copies may continue circulating across multiple platforms.

- **Evidentiary Challenges in Courts**

  The rise of deepfake technology also poses significant challenges for the judicial system. Courts increasingly rely on digital evidence such as photographs, audio recordings, and video footage. However, the existence of highly realistic manipulated media raises concerns regarding the authenticity of such evidence. As deepfake technology becomes more sophisticated, verifying the authenticity of digital evidence may become increasingly difficult.

  This phenomenon has been described by legal scholars Robert Chesney and Danielle Citron as the "liar's dividend," where individuals may dismiss genuine evidence by claiming that it is a deepfake.

10. POLICY RECOMMENDATIONS

Addressing the growing threat of deepfake-enabled cybercrime requires a comprehensive regulatory strategy involving legal reforms, technological safeguards, and institutional cooperation.

- **Enactment of Dedicated Deepfake Legislation**

  One of the most important reforms would be the enactment of specific legislation regulating the creation and distribution of malicious deepfakes. Such legislation should clearly define deepfake technology and establish criminal penalties for its misuse. A risk-based classification system may also be adopted to categorize high-risk deepfake activities such as fraud and large-scale misinformation.

- **Mandatory Labeling of AI-Generated Content**

  Governments may require digital platforms to clearly label synthetic media generated through artificial intelligence. Such labeling mechanisms can help users distinguish manipulated content from authentic media. Several countries have already proposed regulatory measures requiring online platforms to identify and disclose AI-generated content in order to combat misinformation.

- **Strengthening Platform Accountability**

  Technology companies and social media platforms play a crucial role in the spread of deepfake content. Therefore, regulatory frameworks should impose stronger obligations on digital platforms to monitor and remove harmful synthetic media.

These obligations may include:

- Implementation of automated deepfake detection systems
- Rapid takedown procedures for harmful content
- Transparency regarding AI-generated media

- **Development of Deepfake Detection Technologies**

  Investment in technological solutions is essential for combating deepfake misuse. Governments, universities, and technology companies should collaborate to develop advanced detection tools capable of identifying manipulated media. Large datasets and machine-learning techniques are already being used to improve deepfake detection capabilities.

- **Public Awareness and Digital Literacy**

  Technological solutions alone are insufficient to address the challenges posed by deepfake technology. Public awareness and digital literacy programs are equally important. Educational initiatives should teach individuals how to critically evaluate digital content, identify potential misinformation, and verify sources before sharing online media

- **International Cooperation**

  Because deepfake cybercrime often involves cross-border operations, international cooperation is essential. Governments should collaborate through international organizations and cybercrime treaties to share intelligence, harmonize legal standards, and coordinate investigations.

11. CONCLUSION

Deepfake technology represents one of the most significant emerging threats in the field of cybercrime. While artificial intelligence has the potential to drive innovation and technological progress, its misuse in generating manipulated media poses serious risks for privacy, reputation, and digital security.

The analysis presented in this study demonstrates that although existing legal provisions under the Information Technology Act and the Bharatiya Nyaya Sanhita can be applied to certain forms of deepfake misuse, the absence of a dedicated legislative framework creates significant regulatory gaps. Recent judicial decisions indicate that courts have begun addressing deepfake disputes through the doctrines of personality rights and privacy.

However, given the rapid development of artificial intelligence technologies, a more comprehensive regulatory approach is necessary. Strengthening legal frameworks, enhancing technological safeguards, and promoting digital literacy will be essential for protecting individuals from the harmful consequences of deepfake-enabled cybercrime.

12. REFERENCES

1. Ali, M., Fernando, Z., Huda, C., Mahmutarom, M. (2025). Deepfakes and Victimology: Exploring the impact of digital manipulation on victims. *Substantive Justice International Journal of Law*, 8(1).
2. Bhargava, A. (n.d.). Deepfake Technology and it's legal regulation in India: a doctrinal and comparative study. *Vintage Legal.*
3. Bharatiya Nyaya Sanhita, 2023. (India).
4. Boleng, T. K., Rohman, A. (2025). Regulatory gaps and legal enforcement challenges on deepfake pornography as a form of Digital sexual violence in Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(6).
5. China Law Translate. (2022). *Provisions on the Administration of Deep Synthesis Internet Information Services*.
6. Darmawan, M. T., Junaidi A., Khaerudin, A. (2025). Law Enforcement Against Deepfake Abuse in Child Pornography in the Artificial Intelligence Era in Indonesia. *Serambi Hukum Research Journal*, 18(1).
7. Economic Times Legal. (2024). *Delhi HC asks Centre to file report on issue of deepfakes*.
8. European Commission. (2025). *AI Act: Regulatory framework for artificial intelligence*.
9. European Commission. (2025). *Code of practice on transparency of AI-generated content*.
10. Gotora, N. T. (2024). Unmasking deception: Deepfake regulation in the context of South African law, could a rethinking of performers' protection rights be the answer? *International Journal of Law and Information Technology*, Vol. 32.
11. Government of India. (2025, August 8). *India well-equipped to tackle evolving online harms and deepfakes*. Press Information Bureau.
12. Guerrero-Sierra, H. F., Puerta, M.P., Garavito, D. F. (2025). Threats and regulatory challenges of non-consensual pornographic deepfakes: an anlysis of the Colombian case. *Cogent Social Sciences*, 11(1).
13. Indian Kanoon. (2023). *Anil Kapoor v. Simply Life India & Ors.*
14. Information Technology Act, 2000 (India).
15. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
16. International Association of Privacy Professionals. (2025). *Global governance challenges of deepfake technology*.
17. Jain, A. (2025). Deepfakes and misinformation: Legal remedies and legislative gaps. *Indian Journal of Law*, 3(2).
18. Lin, L. S. F. (2025). Organisational challenges in law enforcement's response to AI-driven cybercrime and deepfake fraud. *Laws*, 14(4).
19. LiveLaw. (2025). *Delhi High Court orders take down of YouTube channels hosting deepfake videos of journalist Rajat Sharma*.

20. Ma'arif, A. & et.al. (2025). Social, legal, and ethical implications of AI-generated deepfake pornography on digital paltforms: a systematic literature review. *Social Sciences and Humanities Open*, Vol. 12.
21. Nagumotu, K. (2022). Deepfakes are taking over social media: can the law keep up? *IDEA*, 62(2).
22. Nema, P. (2021). Understanding copyright issues entailing deepfakes in India. *International Journal of Law and Information Technology*, 29(3).
23. Neekhara, P., Dolhansky, B., Bitton, J., & Ferrer, C. C. (2020). Adversarial threats to deepfake detection: A practical perspective. *arXiv Preprint*.
24. Patishman, H. (2025) Global legal actions against AI deepfakes: five laws of 2025. *Regula.*
25. Romero-Moreno, F. (2024). Generative AI and deepfakes: A human rights approach to tackling harmful content. *International Review of Law, Computers and Technology*, 38(3).
26. Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. *Computer Law & Security Review*, 58.
27. Rouse. (2024). *AI-generated deepfakes: What does the law say?*
28. Sandoval, M. P. & et.al. (2024). Threat of deepfakes to the criminal justice system: a systematic review. *Crime Science*, 13(41).
29. Singh, S., & Dhiman, S. (2025). Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges. *MethodsX*, Vol.15.
30. Srikant, M. (2025). Bharatiya laws against deepfake cybercrime: Opportunities and challenges. *Vivekananda International Foundation*.
31. Surasit, N. (2024). Rouge replicants: criminal exploitation of deepfakes in South East Asia. *Global Initiative*.
32. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, Vol. 3.
33. Vaish Associates Advocates. (2026). *Regulation of AI-generated/deepfake content and synthetically generated information in India*.
34. Wang, W., Cai, L., Xiao, T., Wang, Y., & Yang, M. H. (2025). Scaling laws for deepfake detection. *arXiv Preprint*.