

---

## DEEFAKE TECHNOLOGY AND CRIMINAL JUSTICE: ADDRESSING LEGAL AND EVIDENTIARY CHALLENGES

---

Ms. K. Pavithra, B.E., LL.M., Assistant Professor of Law, KMC College of Law, Tirupur

### ABSTRACT

Artificial intelligence has expanded the possibilities of digital content creation, but it has also introduced new forms of criminal misuse. Deepfake technology, which uses artificial intelligence to generate realistic yet fabricated audio, video and images, is one such development. While the technology has several legitimate applications in areas such as entertainment, education and media production, its misuse has become a growing concern for criminal justice systems. Deepfakes have been used to facilitate offences including identity theft, financial fraud, cyber extortion, non-consensual intimate image abuse and the spread of false information. They also pose challenges to the reliability of electronic evidence, making it increasingly difficult to distinguish authentic digital material from manipulated content. This article examines the legal and evidentiary issues associated with deepfake technology from the perspective of criminal justice. It discusses the difficulties faced by investigating agencies in detecting AI-generated content and highlights the role of digital forensic techniques in verifying the authenticity of electronic evidence. The article further considers whether the existing legal framework in India is adequate to deal with offences involving deepfakes and briefly refers to selected international developments that may offer useful guidance. Although several provisions under the current legal framework may be invoked against offences committed through deepfakes, the absence of a specific regulatory approach creates practical challenges in investigation, prosecution and victim protection. The article adopts a doctrinal method based on the analysis of legislation, judicial decisions, government guidelines and academic literature. It argues that responding to crimes involving deepfakes requires more than the application of existing penal provisions. Effective regulation calls for a combination of legal reform, improved forensic capabilities, greater cooperation between technology platforms and law enforcement agencies, and increased public awareness regarding the risks associated with synthetic media. Strengthening these measures is essential to preserve the integrity of digital evidence and to ensure that technological innovation does not weaken the administration of criminal justice.

**Keywords:** Deepfake Technology; Criminal Justice; Artificial Intelligence; Digital Evidence; Digital Forensics; Cybercrime; Synthetic Media; Electronic Evidence; Investigation; Legal Framework.

## 1. INTRODUCTION

Artificial intelligence has considerably influenced the manner in which digital content is created and communicated. Among its various applications, deepfake technology has attracted particular attention because it enables the creation of highly realistic yet fabricated audio, video and image content. By employing artificial intelligence and machine learning techniques, deepfakes can imitate a person's appearance, voice and expressions with remarkable accuracy, making manipulated content difficult to distinguish from authentic recordings. Although the technology has legitimate uses in filmmaking, education, accessibility and digital media, its misuse has become a growing concern.<sup>1</sup> The increasing availability of AI-based tools has made the creation of deepfakes accessible to a wider section of society, resulting in their use for unlawful purposes that affect individuals, institutions and the justice system alike.

The misuse of deepfake technology has introduced new challenges for criminal justice, particularly in relation to investigation and the use of digital evidence. Deepfakes have been employed in offences such as identity theft, financial fraud, cyber extortion, non-consensual intimate image abuse and the dissemination of false information capable of influencing public confidence. At the same time, the growing dependence on electronic records in criminal proceedings has made the authenticity of digital evidence an important legal concern.

Existing laws may be invoked to prosecute many offences committed through deepfakes; however, they do not specifically address several issues arising from AI-generated synthetic media.<sup>2</sup> Against this background, this article examines the criminal risks associated with deepfake technology, analyses the evidentiary and legal challenges arising from its misuse, evaluates the adequacy of the existing Indian legal framework, and suggests measures to strengthen the criminal justice response.

## 2. DEEPAKE TECHNOLOGY AND EMERGING CRIMINAL RISKS

Deepfake technology refers to the use of artificial intelligence to create or alter digital content in a manner that makes fabricated images, videos or audio recordings appear authentic.

---

<sup>1</sup> Henry Ajder, Giorgio Patrini, Francesco Cavalli & Laurence Cullen, *The State of Deepfakes: Landscape, Threats and Impact* (Deeptace Labs, 2019).

<sup>2</sup> Ministry of Electronics and Information Technology, Government of India, *Advisory on Deepfake and AI-Generated Content* (2023).

It generally relies on deep learning techniques, particularly Generative Adversarial Networks (GANs), through which one algorithm generates synthetic content while another evaluates its authenticity until the fabricated output closely resembles the original.<sup>3</sup> Although the underlying technology is complex, the growing availability of user-friendly applications has made the creation of deepfakes possible even without specialised technical knowledge. As a result, synthetic media has become increasingly common across digital platforms, raising concerns about its misuse alongside its legitimate applications.<sup>4</sup>

The technology is not unlawful in itself. Deepfakes have been used in the entertainment industry to recreate historical characters, improve visual effects and facilitate dubbing in different languages. Educational institutions and researchers have also explored their potential for interactive learning, accessibility and historical reconstruction. However, the same technology can easily be employed for deceptive purposes when created or circulated without consent or with an intention to cause harm. The ease with which fabricated content can be produced and shared through social media has significantly increased the risk of misuse, often allowing false information to spread before its authenticity can be verified.

From a criminal justice perspective, deepfakes have become a convenient tool for committing a range of offences. One of the most common forms of misuse involves identity theft, where a person's likeness or voice is manipulated to impersonate them for fraudulent purposes. Artificial intelligence-generated voice recordings have been used to deceive family members, employees and financial institutions into transferring money or revealing confidential information. Deepfakes have also been associated with cyber extortion, online harassment and non-consensual intimate image abuse, causing severe emotional, reputational and financial harm to victims. In addition, fabricated videos and audio recordings have been circulated to spread false information, damage public confidence and influence public opinion during politically sensitive periods. Such misuse demonstrates that deepfakes are capable of causing harm not only to individual victims but also to public institutions and democratic processes.<sup>5</sup>

---

<sup>3</sup> Ian J. Goodfellow, Yoshua Bengio & Aaron Courville, *Deep Learning* (MIT Press, 2016); Yisroel Mirsky & Wenke Lee, "The Creation and Detection of Deepfakes: A Survey," 54(1) *ACM Computing Surveys* (2021).

<sup>4</sup> Henry Ajder, Giorgio Patrini, Francesco Cavalli & Laurence Cullen, *The State of Deepfakes: Landscape, Threats and Impact* (Deeptech Labs, 2019).

<sup>5</sup> Bobby Chesney & Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 107 *California Law Review* 1753 (2019).

The increasing use of deepfakes for criminal purposes has therefore created challenges that extend beyond conventional cybercrime. Unlike traditional digital manipulation, AI-generated synthetic media often leaves very few visible signs of alteration, making detection more difficult for investigators and the general public. This has increased the importance of digital forensic examination and has prompted renewed discussions on whether existing legal mechanisms are capable of addressing offences involving synthetic media. Understanding these risks is essential before examining the challenges that deepfakes pose to criminal investigation and the admissibility of digital evidence.

### **3. CHALLENGES TO CRIMINAL INVESTIGATION AND DIGITAL EVIDENCE**

#### **3.1 Challenges in Criminal Investigation**

The increasing use of deepfake technology presents significant challenges for criminal investigation and the administration of justice. Investigating agencies today rely heavily on electronic records such as CCTV footage, mobile phone recordings, social media content and digital communications to establish facts and identify offenders. The emergence of highly realistic synthetic media has complicated this process by making it more difficult to determine whether a particular recording is genuine or has been manipulated. Unlike traditional forms of digital editing, deepfakes are designed to closely imitate real individuals and events, often leaving few obvious indications of alteration. Consequently, investigators can no longer assume that a digital recording accurately represents the events it appears to depict. Criminal investigations therefore require greater technical scrutiny at every stage, from the collection of evidence to its presentation before the court.<sup>6</sup>

The difficulties extend beyond the detection of manipulated content. Criminal investigations depend upon the collection, preservation and authentication of evidence in a manner that maintains its reliability. Where a deepfake is involved, investigators may require specialised forensic expertise to identify inconsistencies in facial movements, voice patterns, metadata or other digital markers. Such examinations often demand advanced technological tools and trained personnel, resources that may not always be readily available. Delays in detecting fabricated content can affect the course of an investigation and may even result in

---

<sup>6</sup> Yisroel Mirsky & Wenke Lee, "The Creation and Detection of Deepfakes: A Survey," 54(1) *ACM Computing Surveys* (2021).

wrongful suspicion, reputational harm or the diversion of investigative resources.<sup>7</sup>

### 3.2 Challenges Relating to Digital Evidence

Deepfakes raise important concerns regarding the evidentiary value of electronic records before courts. The growing possibility that audio or video recordings may be artificially generated has the potential to weaken public confidence in digital evidence. Parties may challenge the authenticity of electronic records by alleging manipulation, thereby increasing the burden on investigators and forensic experts to establish reliability. This phenomenon is often described as the “liar’s dividend”, where individuals accused of misconduct seek to dismiss genuine recordings as fabricated deepfakes. Such claims can complicate judicial proceedings and make the evaluation of electronic evidence more difficult. As digital evidence has become an integral part of criminal trials, courts must exercise greater caution while assessing its authenticity, relevance and evidentiary value.<sup>8</sup>

### 3.3 Role of Digital Forensics

Digital forensics has become an indispensable component of modern criminal investigations involving deepfakes. Forensic experts assist in examining electronic evidence, identifying signs of manipulation and verifying authenticity through scientific methods. Advanced forensic techniques such as metadata analysis, frame-by-frame examination, facial artefact detection and voice pattern analysis can assist investigators in identifying AI-generated content.<sup>9</sup> However, as deepfake technology continues to evolve, forensic detection methods must also keep pace. Continuous investment in technological infrastructure, specialised training for investigators and standardised procedures for the examination and preservation of electronic evidence are essential to ensure that the criminal justice system remains capable of addressing offences involving synthetic media.

## 4. LEGAL RESPONSES TO DEEPFAKES: THE INDIAN POSITION

### 4.1 Existing Legal Framework

---

<sup>7</sup> Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed., Academic Press, 2011).

<sup>8</sup> *The Bharatiya Sakshya Adhiniyam*, No. 47 of 2023; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

<sup>9</sup> Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed., Academic Press, 2011); Yisroel Mirsky & Wenke Lee, “The Creation and Detection of Deepfakes: A Survey,” 54(1) *ACM Computing Surveys* (2021).

India does not presently have a specific legislation governing deepfake technology or criminalising the creation and dissemination of AI-generated synthetic media. However, this does not mean that offences involving deepfakes fall outside the scope of the law. Depending upon the nature of the offence and the resulting harm, existing provisions under the Bharatiya Nyaya Sanhita, 2023 (BNS) and the Information Technology Act, 2000 (IT Act) may be invoked. Where deepfakes are used for impersonation, financial fraud, dissemination of obscene material, defamation or acts affecting public order, the existing legal framework provides a basis for investigation and prosecution. Nevertheless, these laws were enacted to address broader criminal and cyber offences rather than the unique challenges posed by AI-generated synthetic media.

#### **4.2 Application of the Information Technology Act and the Bharatiya Nyaya Sanhita**

The Information Technology Act, 2000 contains several provisions that may be applied to deepfake-related offences. Identity theft, cheating by personation through computer resources, violation of privacy and the publication or transmission of obscene or sexually explicit electronic content may attract liability under the Act, depending on the circumstances of each case.<sup>10</sup> Similarly, the Bharatiya Nyaya Sanhita, 2023 may be invoked where deepfakes are used to commit offences such as cheating, forgery, criminal intimidation, defamation or the creation of public disorder. In addition, intermediary platforms are required to observe due diligence under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, including taking prompt action against unlawful content upon receiving valid notice and cooperating with investigating agencies.<sup>11</sup> Although these provisions offer legal remedies, their application often depends upon fitting deepfake-related conduct within offences that were originally drafted without artificial intelligence in contemplation.

#### **4.3 Need for a Dedicated Legal Framework**

Despite the availability of existing legal provisions, significant gaps remain in the regulation of deepfakes. The present legal framework primarily addresses the consequences of unlawful conduct rather than the creation, distribution and misuse of AI-generated synthetic media itself. It offers limited guidance on issues such as mandatory disclosure of AI-generated content, forensic standards for authentication, accountability of developers and digital

---

<sup>10</sup> *The Information Technology Act*, No. 21 of 2000, ss. 66C, 66D, 66E, 67 & 67A.

<sup>11</sup> *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, 2021.

platforms, and effective mechanisms for protecting victims from the rapid dissemination of manipulated media.<sup>12</sup> Enforcement also becomes more complex where offences involve anonymous users, encrypted communication or cross-border digital platforms. These limitations suggest that India may benefit from a dedicated legal framework that specifically addresses deepfake technology while balancing technological innovation, freedom of expression and the protection of individual rights.

## **5. STRENGTHENING THE CRIMINAL JUSTICE RESPONSE**

### **5.1 Strengthening the Legal and Institutional Framework**

Addressing offences involving deepfake technology requires a coordinated response that combines legal, technological and institutional measures. While existing laws provide a basis for prosecuting many deepfake-related offences, the increasing sophistication of synthetic media calls for a more structured regulatory approach. A clear legal framework defining the unlawful creation and malicious use of deepfakes would reduce uncertainty in investigation and prosecution while ensuring that legitimate uses of artificial intelligence for education, research and creative expression are not unnecessarily restricted.<sup>13</sup> Such a framework should also establish clear responsibilities for developers, digital platforms and users, while protecting fundamental rights such as freedom of expression and privacy.

### **5.2 Enhancing Investigative and Forensic Capacity**

Strengthening the investigative capacity of law enforcement agencies is equally important. Police officers, prosecutors and forensic experts should receive specialised training to identify and investigate offences involving AI-generated content. Investment in advanced digital forensic tools capable of detecting manipulated audio, video and image files would improve the reliability of criminal investigations and assist courts in assessing the authenticity of electronic evidence. Standard operating procedures for the collection, preservation and examination of digital evidence should also be developed to minimise disputes regarding its admissibility and integrity during criminal proceedings. Regular collaboration between

---

<sup>12</sup> Bobby Chesney & Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 107 *California Law Review* 1753 (2019).

<sup>13</sup> UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

investigating agencies, forensic laboratories and technology experts would further improve the effectiveness of criminal investigations involving deepfakes.<sup>14</sup>

### 5.3 Role of Digital Platforms and Public Awareness

Technology companies and social media platforms must also play an active role in limiting the misuse of deepfakes. The adoption of effective content verification mechanisms, prompt removal of unlawful material and timely cooperation with investigating agencies can significantly reduce the circulation of manipulated content. Public awareness is another essential component of an effective response. Educating users about the existence of deepfakes, methods for identifying suspicious content and the legal remedies available to victims can reduce the likelihood of deception and encourage timely reporting of offences. Since deepfake content frequently crosses national borders, stronger international cooperation in information sharing, investigation and enforcement will also be necessary to ensure that criminal justice systems remain capable of responding effectively to offences involving synthetic media.<sup>15</sup>

## 6. CONCLUSION

Deepfake technology has demonstrated that advances in artificial intelligence can offer significant social and commercial benefits while simultaneously creating new challenges for the criminal justice system. The ability to produce highly convincing fabricated audio, video and images has expanded the scope of offences such as identity theft, financial fraud, cyber extortion and non-consensual intimate image abuse. At the same time, it has raised serious concerns regarding the authenticity and reliability of digital evidence, which has become an indispensable component of modern criminal investigations and judicial proceedings.

Although the existing legal framework in India provides remedies for many offences committed through deepfakes, it does not comprehensively address the unique issues associated with AI-generated synthetic media. As deepfake technology continues to advance, reliance solely on conventional legal provisions may prove inadequate in responding to increasingly sophisticated forms of digital manipulation. An effective response requires not

---

<sup>14</sup> INTERPOL, *Artificial Intelligence and Emerging Crime Trends*; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed., Academic Press, 2011).

<sup>15</sup> Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence* (2019); Ministry of Electronics and Information Technology, Government of India, *Advisory on Deepfake and AI-Generated Content* (2023).

only appropriate legal reforms but also stronger forensic capabilities, trained investigating agencies, responsible conduct by digital platforms and greater public awareness. Collaboration among governments, technology companies, forensic experts and law enforcement agencies will be equally important in addressing the cross-border nature of deepfake-related crimes.

The challenge before the criminal justice system is not to restrict technological progress but to ensure that innovation does not compromise truth, fairness and the rule of law. A balanced legal and institutional framework that protects individual rights while enabling the responsible use of artificial intelligence will preserve public confidence in digital evidence and ensure that justice is not undermined by synthetic media.

Looking ahead, the rapid evolution of artificial intelligence will continue to reshape the nature of cybercrime and digital evidence, requiring criminal justice systems to remain responsive to emerging technological developments. Legal regulation must therefore be supported by continuous advancements in digital forensic science, specialised capacity-building for investigators and prosecutors, and stronger cooperation between governments, technology companies and international agencies. Such a comprehensive and forward-looking approach will enhance the ability of criminal justice institutions to address offences involving deepfakes while safeguarding the rights of individuals and maintaining the credibility of electronic evidence.

Ultimately, a proactive legal and institutional response today is necessary to ensure that artificial intelligence strengthens, rather than undermines, the administration of criminal justice.

## REFERENCES

- Ian J. Goodfellow, Yoshua Bengio & Aaron Courville, *Deep Learning* (MIT Press, 2016).
- Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn., Pearson, 2022).
- Bobby Chesney & Danielle Keats Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,” (2019) 107 *California Law Review* 1753.
- Yisroel Mirsky & Wenke Lee, “The Creation and Detection of Deepfakes: A Survey,” (2021) *ACM Computing Surveys*. NITI Aayog, *National Strategy for Artificial Intelligence* (2018).
- Ministry of Electronics and Information Technology (MeitY), Government of India, Advisory on Deepfake and AI-Generated Content (2023).
- The Constitution of India, 1950.
- The Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).
- The Information Technology Act, No. 21 of 2000 (India).
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under the Information Technology Act, 2000.
- The Digital Personal Data Protection Act, No. 22 of 2023 (India).
- The Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India).