Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Deepfakes as a Tool for Criminal Activity

Tania Kukreja[a]

[a]Amity University, Mohali, India

Received 22 May 2025; *Accepted* 23 June 2025; *Published* 27 June 2025

Deepfake technology, an advanced form of artificial intelligence that creates hyper-realistic but fabricated audio-visual content, has rapidly evolved into a potent tool for criminal activity. This paper focuses on the criminal misuse of deepfakes, highlighting notable cases involving financial fraud, political misinformation, and privacy violations. Despite the alarming rise in deepfake-related crimes reported to have surged by over 550% since 2019, with projected losses reaching ₹70,000 crore in 2024, India currently lacks specific legislation addressing this threat. Existing laws under the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita 2023 provide partial remedies but fall short of comprehensively tackling deepfake-enabled offences. Through an analysis of landmark Indian cases such as the Kerala deepfake scam and the Anil Kapoor deepfake pornography case, this study examines the socio-legal challenges posed by deepfakes. It further compares India's regulatory landscape with countries like the European Union, which has introduced the Digital Services Act mandating the swift removal of harmful synthetic media. The paper argues for urgent legislative reforms, enhanced forensic capabilities, and public awareness initiatives to effectively combat deepfake crimes in India. This focused inquiry aims to contribute to the evolving discourse on safeguarding individual rights and democratic processes against the growing menace of AI-driven synthetic media.

Keywords: *deepfake crime, artificial intelligence, cybercrime, ipc, legal reform.*

INTRODUCTION

The advancement of technology has not only transformed traditional crime but has also given rise to new forms of criminal activity. Among these, cyber-related crimes have experienced a significant evolution. Computer-related offences are now more complex than ever, particularly with the emergence of artificial intelligence (AI) technologies, notably deepfake technology.

Deepfake technology utilises AI to create hyper-realistic synthetic media and has witnessed a rapid increase in both use and sophistication. While it has opened avenues for creative expression, the potential for misuse has raised significant ethical and legal concerns. Deepfake fraud accounts for 40 percent of all AI-related cybercrimes worldwide, in addition to other threats like cybercrime automation and AI-driven privacy violations. In 2024, there have been over one million reported deepfake videos, and more than 50 applications exist for producing such content, highlighting the ease of access to these tools.[1]

In the political arena, deepfakes have been employed to disseminate misinformation, exemplified by the manipulated videos. One such example is from early 2022, when a deepfake video of the Ukrainian president Volodymyr Zelenskyy came out in which he was seen as 'urging' the Ukrainian fighters to lay down arms and surrender to Russia. Another such example is of mid-2023, when a presidential campaign advertisement for Republican candidate Ron DeSantis featured deepfake still images depicting his rival, President Donald Trump, in an embrace with Dr. Anthony Fauci. Fauci is regarded as a contentious figure by many Republican voters.[2] Such occurrences have underscored the risks deepfakes pose to democratic processes and public trust.

In the entertainment sector, there are alarming instances of unauthorised deepfake applications, such as the non-consensual use of celebrities' faces on adult film actors, leading to serious breaches of privacy. Additionally, deepfake technology has been utilised to perpetrate fraud, as demonstrated by a notable case in late 2019 where a company was

[1] 'India's Deepfake Cases Up 550%, Losses May Hit Rs 70,000 Cr By 2024: Report' *Business World* (05 December 2024) <https://www.businessworld.in/article/indias-deepfake-cases-up-550-losses-may-hit-rs-70000-cr-by-2024-report-541202> accessed 18 May 2025

[2] Dan Cavedon-Taylor, 'Deepfakes: a survey and introduction to the topical collection' (2024) 204 Synthese <https://link.springer.com/article/10.1007/s11229-024-04634-8> accessed 18 May 2025

defrauded of nearly $200,000 due to attackers using deepfake audio to impersonate the voice of a CEO of a UK-based energy firm.[3]

The social implications of such deepfakes extend even further, as the generation of fake news has led to social unrest and distrust among society towards legitimate media sources. As this technology is becoming more accessible, there is a need to enhance the digital literacy skills among the public to notice the genuine content from the manipulated media.

Responses to the challenges posed by deepfakes are still developing, with some countries beginning to draft legislation aimed at mitigating risks associated with their misuse. However, the rapid evolution of technology poses a notable challenge for lawmakers, who must adapt swiftly to keep pace with new developments. While deepfake technology has the potential to revolutionise various fields through artistic and communicative enhancements, its misuse poses severe risks that cannot be overlooked. As illustrated by recent cases, the implications of deepfakes extend beyond deception; they threaten individual safety, privacy, and societal norms. Thus, a collaborative effort among technologists, policymakers, and the public is essential to navigate the complexities and challenges presented by this powerful tool.

This paper provides a focused analysis of deepfake technology as a tool for criminal activity in India. It defines deepfakes and the AI techniques behind them, such as machine learning and GANs. The paper explores their use in misinformation, identity theft, and fraud through recent Indian and global cases. It highlights the risks deepfakes pose and examines the limitations of existing Indian laws, including the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, in addressing these challenges. A comparative review of regulations like the EU's Digital Services Act is included to suggest reforms. The study calls for urgent legislative and enforcement measures to combat deepfake crimes effectively in India.

UNDERSTANDING DEEPFAKE TECHNOLOGY AND ITS CRIMINAL USE

Deepfakes are a form of synthetic media produced using AI techniques, wherein video or audio is manipulated to appear authentic, featuring people who seem to say or do things

[3] *Ibid*

they have never actually said or done.[4] Deepfake technology uses advanced machine learning techniques, primarily involving **generative adversarial networks (GANs)** and autoencoders, to create realistic fake audio or video content. These tools analyse the facial features, voice patterns, and movements to create high-quality fake videos or images which look real. The GAN consists of 2 algorithms:

- **The Generator** creates fake content based on the real data present.
- **The Discriminator** assesses the degree to which the fake resembles real examples in terms of credibility.

The generator continuously enhances its output by utilising feedback from the discriminator. This ongoing interaction ultimately enables the system to generate increasingly realistic and believable deepfakes.

To produce a deepfake, a GAN initially examines images or videos of an individual from different perspectives to grasp their facial features, movements, and expressions. For video content, it also evaluates speech and behavioural traits. The generator subsequently produces synthetic content, while the discriminator fine-tunes it until the final result closely mimics authentic footage. The deepfake videos are created in 2 methods. One is source video manipulation, where the existing video is altered, and the other is face swapping, where one person's face is replaced by another person's face.[5]

Furthermore, the rise of **Crime as a Service (CaaS)** alongside deepfake technology is a growing concern for law enforcement because deepfakes can help with various criminal activities, such as:[6]

- Harassing or shaming individuals on the internet;
- Engaging in extortion and fraudulent activities;
- Enabling document forgery;
- Creating fake online identities and deceiving 'know your customer' protocols;

[4] 'Tackling Deepfakes in European Policy' (*European Parliament*, 30 July 2021) <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf> accessed 18 May 2025

[5] 'What Is Deepfake Technology? A Comprehensive Guide for 2025' (*Bestarion*, 07 May 2025) <https://bestarion.com/what-is-deepfake-technology/> accessed 18 May 2025

[6] Cornelia Riehle, 'Europol Report Criminal Use of Deepfake Technology' (*Eucrim*, 09 May 2022) <https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/> accessed 18 May 2025

- Distributing non-consensual explicit content;
- Exploiting children online;
- Tampering with or falsifying electronic evidence in criminal investigations;
- Disrupting financial markets;
- Spreading misinformation and swaying public opinion;
- Aiding extremist or terrorist group narratives;
- Fuelling social unrest and political division.

Financial Fraud and Impersonation: Deepfakes have enabled a new wave of sophisticated financial crimes. A striking example is the 2024 Arup case in the UK, where fraudsters used deepfake video and audio to impersonate senior executives during a video call, deceiving an employee into transferring $25 million to criminal accounts. This was not an ordinary cyberattack that breached a company's digital infrastructure. Instead, it employed psychological tactics and advanced deepfake technology to manipulate the employee's trust.[7] Like this, similar scams have been reported globally, with deepfake voices and videos used to authorise fraudulent transactions or manipulate business operations.

Identity Theft and Social Engineering: Criminals use deepfakes to bypass digital identity verification systems, such as video KYC (Know Your Customer) protocols. In a notable attack on an Indonesian financial organisation, over 1,100 deepfake attempts were made to defeat biometric security and gain unauthorised access. This poses a risk to the integrity of digital identity verification utilised in passport applications, social security systems, and various online services. The capability to generate realistic video responses in real-time specifically undermines existing biometric security measures and video verification protocols.[8]

Political Manipulation and Disinformation: Deepfakes have been weaponised to spread misinformation and manipulate public opinion, especially during elections. The incident involving an AI-generated robocall that impersonated Joe Biden and urged Democrats not to

[7] *Ibid*
[8] '8 Deepfake Threats to Watch in 2025' (*MEA*, 13 January 2025) <https://www.mea-integrity.com/8-deepfake-threats-to-watch-in-2025/> accessed 18 May 2025

participate in the New Hampshire Democratic primary in January is just one among numerous examples of deepfakes being employed for electoral fraud.[9]

Non-Consensual Content and Harassment: A significant proportion of deepfakes online are used to create non-consensual pornography, often targeting celebrities and private individuals. In a significant case in India, a 76-year-old man was targeted by cybercriminals who utilised a deepfake video featuring the face and voice of a retired IPS officer. The criminals extorted money from him, claiming he was soliciting sex, which led the elderly man to make repeated payments out of fear that police would take action against him. This incident represents one of the first known instances in India where deepfake technology was used for such malicious purposes, severely impacting the victim's emotional state and leading him to contemplate suicide before he finally involved his family and law enforcement.[10]

Another notable case is that of journalist Rana Ayub, where deepfake technology was misused to clone her identity for harassment. Her images were manipulated and circulated online, raising significant concerns about privacy violations and the psychological impact on the victims.[11]

In 2023, Bollywood actor Anil Kapoor expressed his dissatisfaction when certain websites used deepfake technology to feature his face and his famous 'Jhakaas' catchphrase in inappropriate advertisements and videos without his consent. The Delhi High Court ruled that this constituted a violation of his personality rights and ordered the sites to cease such activities. This case underscored the risks posed by deepfakes in misleading the public and harming the reputations of celebrities.[12] Numerous similar incidents have occurred involving

[9] 'Top 5 Cases of AI Deepfake Fraud From 2024 Exposed' (*Incode,* 20 December 2024) <https://incode.com/blog/top-5-cases-of-ai-deepfake-fraud-from-2024-exposed/> accessed 18 May 2025

[10] 'Man Gets Caught in Deepfake Trap, Almost Ends Life; among First Such Cases in India' *The Economic Times* (30 November 2023) <https://economictimes.indiatimes.com/news/new-updates/man-gets-caught-in-deepfake-trap-almost-ends-life-among-first-such-cases-in-india/articleshow/105611955.cms> accessed 18 May 2025

[11] Debarati Halder and Subhajit Basu, 'Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India' (2025) 34(2) Information and Communications Technology Law <https://www.tandfonline.com/doi/pdf/10.1080/13600834.2024.2408914> accessed 18 May 2025

[12] Pratyusha Satpathy, 'Deepfakes And The Law: Fighting AI Fakery And Protecting Image Rights In India' (*Lawful Legal*, 06 May 2025) <https://lawfullegal.in/deepfakes-and-the-law-fighting-ai-fakery-and-protecting-image-rights-in-india/> accessed 18 May 2025

actors and public figures whose faces or voices have been used without their permission to create inappropriate advertisements or videos.

Amidst these disturbing developments, India's Cyber Crime Coordination Centre (I4C) has reported a 300% increase in deepfake-related complaints from early 2023 to late 2024, emphasising the growing threat of non-consensual content in the digital landscape.[13]

Evidence Manipulation and Legal Risks: Deepfakes pose a direct threat to the integrity of digital evidence in legal proceedings. Fabricated audio, video, or documents can be presented in courtrooms, challenging the authenticity of evidence and complicating judicial processes. Law enforcement agencies now face the dual challenge of detecting deepfakes and ensuring that genuine digital evidence can be trusted.[14] One notable case highlighting the implications of deepfake technology occurred during the custody dispute in the UK, where an attorney successfully challenged audio evidence that had been revealed as a deepfake, undermining the credibility of what seemed to be incriminating material against a party involved.[15] This incident illustrates how deepfake technology can be leveraged to create misleading evidence, prompting courts to question the authenticity of recordings presented during trials.

LEGAL FRAMEWORK IN INDIA ADDRESSING DEEPFAKE CRIMES

Currently, India lacks specific legislation targeting deepfakes, relying instead on fragmented provisions under existing laws such as the Information Technology Act, which addresses privacy violations and impersonation but does not explicitly cover deepfake technology, thereby creating a legal grey area that hampers effective prosecution.[16]

Such acts are prosecuted under:

[13] Sandeep Jadhav, 'India's Deepfake Problem: Can You Still Trust What You See?' (*Pulse Wire,* 15 May 2025) <https://pulsewire.in/indias-deepfake-problem-2025/> accessed 18 May 2025
[14] *Ibid*
[15] Gurjot Singh, '"Offending Sentiments", A Developing Ground Limiting Free Speech' (*Live Law,* 20 June 2025) <https://www.livelaw.in/articles/offending-sentiments-developing-ground-limiting-free-speech-295364> accessed 20 June 2025
[16] Niranj Ajith Milana, 'Legal Risks of Deepfakes and AI Evidence Manipulation' (*Law Reporters,* 16 June 2025) <https://thelawreporters.com/when-ai-becomes-a-loophole-legal-risks-of-deepfake-deception-and-digital-evidence-manipulation> accessed 20 June 2025

Information Technology Act 2000 –

Section 66D: Punishment for identity fraud and online impersonation with AI-generated deepfakes includes up to 3 years in prison and a fine of up to ₹1 lakh.[17]

Section 67: Posting offensive material electronically makes it a crime to share sexually explicit or offensive deepfake videos. The punishment can be up to 5 years in prison and a fine of up to ₹10 lakh.[18]

Section 69A: The government has the authority to restrict public access to information, enabling it to block deepfake content that poses a threat to national security, sovereignty, or public order.[19]

Section 72: Breach of confidentiality and privacy occurs when a deepfake infringes on an individual's privacy by distributing manipulated private images or videos. The punishment can be up to 2 years in prison and a fine.[20]

Indian Penal Code 1860 –

Section 499 of the Indian Penal Code[21] is now BNS Section 196[22]. This section defines defamation and stipulates the punishment for it.

Punishment: Up to 2 years of imprisonment, a fine, or both.

Section 292 of the Indian Penal Code[23] is now BNS Section 187[24] for acts or materials that are considered obscene.

Section 354A & 354D: Sexual Harassment & Cyber Stalking, applies when deepfakes are used to harass individuals, especially women (e.g., morphing images into obscene content).[25]

Punishment: 3 years imprisonment (for 354A) and up to 5 years (for 354D).

[17] Information Technology Act 2000, s 66D
[18] Information Technology Act 2000, s 67
[19] Information Technology Act 2000, s 69A
[20] Information Technology Act 2000, s 72
[21] Indian Penal Code 1860, s 499
[22] Bharatiya Nyaya Sanhita 2023, s 196
[23] Indian Penal Code 1860, s 292
[24] Bharatiya Nyaya Sanhita 2023, s 187
[25] Indian Penal Code 1860, ss 354A and 354D

Section 420: Cheating & Fraud, if a deepfake is used for financial fraud, identity theft, or scams, this section applies.[26]

Punishment: Up to 7 years of imprisonment and a fine.

The **Bharatiya Nyaya Sanhita, 2023 (BNS**), has incorporated section 111(1), which defines 'organised crime' to include cybercrimes with 'severe consequences,' but fails to explicitly address deepfakes or provide procedural mechanisms for investigation.[27]

Other Relevant Laws –

Indecent Representation of Women (Prohibition) Act 1986: It bans the publication of morphed images/videos of women.

Representation of the People Act 1951 (Election-related Deepfakes): If deepfakes are used to spread fake political propaganda, it can be challenged under this law.

The Digital Personal Data Protection Act 2023 (Privacy Violations) protects against unauthorised use of personal data in AI-generated deepfakes.

Challenges with the Indian Provisions are –

Lack of AI-Forensic Tools for Police: Indian law enforcement agencies face significant technical limitations in detecting and tracing deepfakes. Most police and cybercrime units lack access to advanced AI-based forensic tools and the specialised training required to identify manipulated audio, video, or images. This results in delayed investigations, weak enforcement, and a low conviction rate for deepfake-related crimes. The sophistication and rapid evolution of deepfake technology further widen the gap between perpetrators and investigators, making it difficult to keep pace with new methods of deception.[28]

[26] Indian Penal Code 1860, s 420
[27] Vaishnavi Singh, 'Dissecting The Conundrum Of Deepfake Technology And Artificial Intelligence In Light Of The New Penal Laws Of India' (*Cell for Law and Technology*) <https://clt.nliu.ac.in/?p=1097> accessed 18 May 2025
[28] Zeeshan Shaikh et al. 'Exploring Legal and Technical Challenges of Deepfake in India' (2025) 13(6) International Journal for Research in Applied Science & Engineering Technology <https://www.ijraset.com/best-journal/exploring-legal-and-technical-challenges-of-deepfake-in-india> accessed 18 May 2025

No Mandatory Takedown Timelines for Platforms: Currently, India does not have a uniform, legally mandated timeline for digital platforms (such as Meta, YouTube, or X) to remove deepfake content once reported. While the IT Rules, 2021, require intermediaries to act on user complaints, enforcement is inconsistent and often slow. The lack of a clear, enforceable deadline allows harmful deepfake content to remain online for extended periods, increasing the risk of reputational damage, financial loss, and public misinformation.[29] In contrast, jurisdictions like the European Union mandate the takedown of illegal synthetic content within 24 hours, ensuring faster response and greater accountability.

Cross-Jurisdictional Coordination Issues: Many deepfake crimes involve perpetrators operating from different states or even outside India, complicating investigation and prosecution. For example, in the Kerala-Gujarat fraud case, funds and digital evidence were traced across state borders, requiring coordination between multiple law enforcement agencies. When deepfake servers or creators are located overseas, extradition and cross-border legal cooperation become even more challenging. This international dimension makes it difficult to identify suspects, gather evidence, and enforce Indian laws effectively.[30]

Enforcement Difficulties: India faces significant enforcement hurdles in combating deepfake crimes. Law enforcement agencies often lack advanced AI forensic tools and technical expertise to reliably detect or trace deepfake content, which leads to delayed investigations and weak enforcement. The anonymity of perpetrators—often operating from foreign jurisdictions or using sophisticated anonymisation techniques—complicates identification and prosecution. Cross-border jurisdictional issues further hinder effective legal action, as many deepfake servers and creators are located outside India, making extradition and evidence collection challenging. Courts also struggle with the admissibility and verification of digital evidence, sometimes requiring forensic AI experts to determine authenticity.[31]

---

[29] 'Deepfake: India Addresses Deepfake Threats: Calls for Legal Action and Tech Solutions' *The Economic Times* (09 November 2023) <https://economictimes.indiatimes.com/opinion/et-editorial/india-addresses-deepfake-threats-calls-for-legal-action-and-tech-solutions/articleshow/105103198.cms?from=mdr> accessed 18 May 2025

[30] Nikita Agarwal, 'Legal Challenges Of Deepfake Technology And Ai-Generated Content In India' (*Jus Corpus,* 21 April 2025) <https://www.juscorpus.com/legal-challenges-of-deepfake-technology-and-ai-generated-content-in-india/> accessed 18 May 2025

[31] *Ibid*

Need for Digital Literacy and Public Awareness: A significant portion of the population remains unaware of deepfake threats and how to identify manipulated content. Public awareness campaigns and digital literacy initiatives are essential to empower citizens to recognise, report, and protect themselves against deepfake-related harms. Government and cybersecurity organisations are increasingly launching such programs, but coverage and effectiveness need to be scaled up.[32]

Pending Reforms –

Acknowledging the challenges associated with deepfakes, the Ministry of Electronics and Information Technology (MeitY) presented a report in 2025 that recommends several important reforms:

Legal Definition of Deepfakes: The report calls for the establishment of a precise legal definition of deepfakes within Indian law. By explicitly defining deepfakes, it will be easier to address existing legal gaps, facilitating the prosecution of offenders and regulating the production, distribution, and use of synthetic media.

Mandatory 24-Hour Takedown for Platforms: MeitY suggests the introduction of a legal obligation for digital platforms to remove reported deepfake content within 24 hours, akin to the provisions of the EU's Digital Services Act. This measure aims to ensure prompt action against harmful content, thereby minimising the potential harm caused by such media.

Digital Watermarking of AI-Generated Content: The report advocates for the requirement of digital watermarking or labelling for AI-generated media. This initiative would enable users and authorities to differentiate between genuine and synthetic content, thereby enhancing traceability and accountability for those who create and distribute deepfakes.

COMPARATIVE ANALYSIS: INDIA AND OTHER JURISDICTIONS

The European Union has introduced its first Artificial Intelligence Act ('EU AI Act'), which addresses the regulation and usage of AI, including necessary guidelines for deepfakes. In 2023, the UK government implemented reforms to its Online Safety Act, marking the first

[32] 'Real or Fake? Dealing with Deepfakes Dilemma in Digital Society' (*Anand & Anand*, 04 February 2025) <https://www.anandandanand.com/news-insights/real-or-fake-dealing-with-deepfakes-dilemma-in-digital-society/> accessed 18 May 2025

instance of criminalising the sharing of deepfake intimate images. It also made amendments to its Criminal Justice Bill, establishing penalties for creating horrific images without consent. Similarly, the United States has introduced the Deepfakes Accountability Bill in 2023, while China has enacted the Artificial Intelligence Law of the People's Republic of China, both of which mandate labelling deepfakes on online platforms, with noncompliance leading to potential criminal sanctions.[33]

India's Approach –

India currently addresses deepfake-related crimes through a patchwork of existing laws, including the Information Technology Act 2000, the Bharatiya Nyaya Sanhita 2023, and the Digital Personal Data Protection Act 2023. These laws cover issues like privacy violations, defamation, and cyber fraud, but none specifically define or comprehensively regulate deepfakes. Enforcement relies on broad provisions such as Section 66E (privacy violation), Section 67 (obscenity), and relevant sections of the BNS for forgery and defamation. The government has issued advisories to social media platforms, requiring them to remove reported deepfake content within 36 hours under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021. However, there is no dedicated deepfake law, and the absence of clear definitions or AI-specific offences creates significant legal ambiguity and enforcement challenges.[34]

Judicial innovation has sought to address certain gaps, as illustrated in the case of Bhavna Sharma v Union of India. In this instance, the Delhi High Court contemplated the possibility of prohibiting access to platforms that generate deepfakes but ultimately hesitated due to worries over freedom of expression and the lack of explicit statutory authority. While courts have acknowledged issues related to personality rights and privacy in deepfake cases, the responses have been fragmented rather than constituting a comprehensive regulatory framework.[35]

---

[33] Singh (n 16)

[34] 'Navigating the Evolving Landscape of Deepfake Laws: A Guide for Online Platforms and Businesses' (*Social Media Matters*) <https://www.socialmediamatters.in/our-work/online-safety/evolving-landscape-of-deepfake-laws> accessed 18 May 2025

[35] Sidharth Chopra et al., 'Artificial Intelligence 2025 - India | Global Practice Guides' (*Chambers and Partners*, 22 May 2025) <https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2025/india/trends-and-developments> accessed 18 May 2025

European Union[36] -

The European Union has taken a proactive and comprehensive approach to deepfake regulation through the EU Artificial Intelligence Act (AI Act) and the Digital Services Act (DSA). Key features include:

Transparency and Labelling: The AI Act requires that all AI-generated or manipulated content, including deepfakes, be clearly labelled as such. This helps users recognise synthetic content and reduces the risk of deception.

High-Risk Classification: Deepfakes used for political manipulation, defamation, or other malicious purposes are classified as 'high-risk,' subjecting them to stricter oversight and compliance requirements.

Traceability: The law mandates that creators and deployers of deepfakes maintain records of the data and processes used, enabling authorities to trace the origins of harmful content.

Swift Takedown Requirements: The DSA requires platforms to remove illegal deepfake content within 24 hours of notification, ensuring rapid response and minimising harm.

Severe Penalties: Non-compliance can result in fines up to 35 million euros or 7% of global annual turnover.

United States[37] –

The United States lacks a unified federal law on deepfakes, but several states, such as Texas, California, and New Jersey, have enacted specific statutes:

Election Integrity: Laws prohibit the creation or distribution of deepfakes intended to influence elections within a certain period before voting.

Criminalisation of Malicious Deepfakes: Some states criminalise the non-consensual creation or distribution of deepfake pornography or deepfakes used for fraud and harassment.

[36] *Ibid*
[37] Agarwal (n 30)

Penalties: Offenders can face significant fines and imprisonment, with the severity depending on the harm caused.

China –

China has implemented some of the world's strictest regulations on deepfakes:

Mandatory Labelling: All synthetic content must be clearly labelled

Prohibition of Harmful Deepfakes: Content that threatens national security, social stability, or individual rights is strictly prohibited.

Platform Accountability: Platforms are required to detect, label, and promptly remove deepfake content.

KEY DIFFERENCES AND LESSONS FOR INDIA

Aspect	**India**	**European Union**	**United States (States)**	**China**
Dedicated Law	No	AI Act, DSA	In some states	National regulations
Definition	Not defined	Clearly defined in law	Defined in state laws	Defined in regulations
Labelling	Not mandatory	Mandatory labelling and transparency	Not uniform	Mandatory
Takedown	36 hours (advisory, not statutory)	24 hours (statutory)	Varies by state	Immediate
Penalties	Patchwork (IT Act, BNS, DPDPA)	Severe financial penalties	Fines, imprisonment (state-specific)	Severe, including

				platform liability
Scope	Reactive, case-by-case	Proactive, comprehensive	State-level, fragmented	National, strict

GLOBAL CHALLENGES AND SOCIO-LEGAL IMPLICATIONS

Though the use of deepfake was done as an advancement of technology in many sectors, like:[38]

- In entertainment and media production, where deepfakes are used frequently to de-age the actors or recreate the deceased one in the films, making facial expressions for animated characters, etc., these are done to save time and budget while not compromising on the creative factor.
- In social media and viral content where platforms use deepfakes often use such videos or images to create humorous and entertaining content for people to see.
- The use of deepfake in marketing and advertising creates a global reach for their brand and is more personalised.
- Used in academic and corporate training. It creates an immersive learning experience. From historical enactments to realistic role-playing simulations to virtual tutors, explain the material in different languages and voices. It creates a wholesome experience for learning and training.

There are numerous instances where deepfakes contribute positively to education and personal development; however, unfortunately, many individuals are leveraging this technology for harmful purposes, including:

Fabrication of Evidence: The courts face difficulty in verifying the authenticity of audio and video evidence. The advancements in deepfake technology can lead to highly convincing yet fabricated content, making it increasingly arduous for judicial systems to discern real from artificially generated media. This situation often necessitates the involvement of **digital forensic experts and advanced tools**, such as digital certificates and verification technologies

[38] What Is Deepfake Technology? A Comprehensive Guide for 2025 (n 5)

like Microsoft's Video Authenticator, to authenticate the evidence presented in court. In India, the admissibility of electronic records is done under Section 65 B of the Indian Evidence Act. Without such interventions, the integrity of legal proceedings can be compromised, potentially resulting in wrongful convictions or acquittals.[39]

Detection Complexity: The sophistication of deepfake technology makes it increasingly difficult to reliably detect and attribute manipulated content to its creators. Even advanced forensic tools struggle to keep pace with rapidly evolving AI models, resulting in significant challenges for law enforcement and judicial systems worldwide.[40]

Impact on Democracy, Privacy, and Public Trust –

Political Interference: Deepfakes have been used to manipulate elections and undermine democratic institutions by spreading misinformation and fabricating statements from political figures. This can sway public opinion and erode trust in democratic processes, as seen in several high-profile global incidents.

Social Engineering and Fraud: Deepfakes facilitate advanced social engineering attacks, such as impersonating executives to authorise fraudulent transactions or bypassing identity verification systems. For instance, face swap attacks on ID verification systems surged by 704% in 2023, and a Hong Kong finance worker was tricked into transferring $25 million after a deepfake video call with 'fake' executives[41].

Privacy Violations and Harassment: The creation of non-consensual deepfake pornography and other forms of digital harassment has become a widespread issue, leading to psychological harm, blackmail, and reputational damage. Laws like Australia's Criminal Code Amendment (Deepfake Sexual Material) Act have been introduced to address such harms.[42]

---

[39] Satpathy (n 12)
[40] Sophie Li, 'Navigating the Deepfake Dilemma: Legal Challenges and Global Responses' (*Rouse,* 13 June 2025) <https://rouse.com/insights/news/2025/navigating-the-deepfake-dilemma-legal-challenges-and-global-responses> accessed 20 June 2025
[41] Laura Fitzgerald, 'Deepfake Trends to Look Out for in 2025' (*Pindrop*, 01 April 2025) <https://www.pindrop.com/article/deepfake-trends/> accessed 18 May 2025
[42] Claudia Koon Ghee Wee, 'Artificial Illusion: Global Governance Challenges of Deepfake Technology' (*IAPP,* 23 April 2025) <https://iapp.org/news/a/artificial-illusion-global-governance-challenges-of-deepfake-technology> accessed 18 May 2025

Erosion of Public Trust: As deepfakes become more prevalent, public scepticism towards digital content grows. Studies show that a significant portion of consumers and business leaders are concerned about the reliability of online information, with many struggling to distinguish between real and AI-generated media.[43]

Regulatory and Governance Challenges[44] –

Lagging Legislation: Most countries' legal frameworks have not kept pace with the rapid evolution of deepfake technology. While some jurisdictions (EU, China, Australia, Singapore) have enacted specific regulations, many others still rely on outdated or piecemeal laws.

Platform Responsibility: Governments are increasingly requiring digital platforms to detect, label, and remove deepfake content. The EU's Digital Services Act and China's regulations mandate swift takedowns and transparency, but enforcement and compliance remain inconsistent globally.

Corporate and Industry Gaps: Many enterprises recognise the risks but lack comprehensive mitigation strategies. For example, only 29% of firms have taken steps to protect against deepfake threats, and less than half have any mitigation plan in place.

Societal and Ethical Implications[45] –

Media Literacy and Awareness: The general public often lacks the skills to identify deepfakes, making media literacy and digital education crucial. Awareness campaigns and critical evaluation of digital content are essential to mitigate the spread and impact of misinformation.

Innovation vs Regulation: Striking a balance between fostering AI innovation and ensuring robust safeguards against misuse remains a pressing challenge. Flexible, adaptive regulatory frameworks are needed to address emerging risks without stifling technological progress.

---

[43] Michael Steinhart et al., 'Deepfake disruption: A cybersecurity-scale challenge and its far-reaching consequences' (*Deloitte Insights,* 19 November 2024) <https://www.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2025/gen-ai-trust-standards.html> accessed 18 May 2025

[44] Chopra (n 35)

[45] Steinhart (n 43)

CONCLUSION

Deepfake technology has rapidly emerged as a formidable tool for criminal activity, presenting unprecedented challenges for legal systems, law enforcement, and society at large. In India, the surge in deepfake-related crimes—ranging from financial fraud and identity theft to political manipulation and non-consensual content—has exposed significant gaps in the existing legal and enforcement framework. While provisions under the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, offer partial remedies, they are inadequate to address the unique complexities and evolving nature of AI-generated synthetic media.

Globally, countries like the European Union, the United States, and China have begun implementing dedicated regulations that mandate transparency, swift takedown of harmful content, and severe penalties for non-compliance. These international approaches highlight the need for India to move beyond a reactive, fragmented strategy toward a comprehensive, proactive legal framework that specifically defines and criminalises malicious deepfake activities.

The socio-legal implications of deepfakes are far-reaching: they threaten democratic institutions, erode public trust, violate privacy, and can cause irreparable harm to individuals and communities. Addressing these challenges requires a multi-pronged approach—combining robust legislation, investment in forensic AI capabilities, mandatory watermarking and transparency for AI-generated content, and widespread public digital literacy initiatives.

As deepfake technology continues to advance, India must prioritise urgent legal reforms, foster multi-stakeholder cooperation, and invest in technological solutions to safeguard individual rights and the integrity of public discourse. Only through such coordinated and adaptive measures can the nation effectively combat the growing menace of deepfake-enabled crime and ensure a secure digital future.