International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Deepfakes and Digital Deception: A Study of India's Legal Preparedness

Ritik Srivastava

Assistant Professor, Shambhunath Institute of Law, Prayagraj

ABSTRACT

The rapid advancement of artificial intelligence and digital media technologies has led to the emergence of digital deception and deepfakes, a form of synthetic media capable of convincingly manipulating images, videos and audio. While this technology has beneficial applications in entertainment, education and digital content creation, it also poses significant risks in the form of misinformation, identity theft, reputational damage and political manipulation. This paper examines the concept of deepfakes and digital deception from the Indian perspective and evaluates the extent to which the existing legal framework is prepared to address these emerging challenges. The study analyzes relevant provisions and laws such as the Information Technology Act, 2000, the Bhartiya Nyaya Sanhita, 2023 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to assess their effectiveness in regulating the misuse of deepfake technology and addressing digital deception. Furthermore, the research highlights existing legal gaps and enforcement challenges in dealing with AI-generated synthetic media. This paper aims to contribute to the ongoing discourse on strengthening legal and regulatory responses to safeguard digital integrity, individual rights and public trust in the digital age.

KEYWORDS: Deepfake; Digital Deception; Artificial Intelligence; Synthetic Media; Digital Media Technology

INTRODUCTION

The rapid growth of digital technologies and artificial intelligence has significantly transformed the way information is created, shared and consumed in contemporary society. With the increasing accessibility of advanced machine learning tools, new forms of manipulated media have emerged, raising serious concerns about authenticity and trust in digital communication. Among these developments, deepfakes and other forms of digital deception have become prominent challenges in the modern digital ecosystem. Deepfakes refer to AI-generated or AI-manipulated audio, video or images that convincingly depict individuals saying or doing things that they never actually said or did. Because of their highly realistic appearance, such synthetic media can easily mislead viewers and spread false narratives. Digital deception, which involves the deliberate use of digital technologies to mislead, manipulate or deceive individuals or groups, is one of the most significant concerns in the modern digital era. Digital deception refers to the creation, alteration or dissemination of false or misleading information through digital platforms in order to influence perceptions, opinions or actions. It can take many forms, including manipulated images and videos, fabricated news articles, fake social media accounts, phishing schemes and other forms of online fraud.

The growing use of social media platforms and digital communication channels has further amplified the reach and potential impact of manipulated content. In recent years, deepfake technology has been used not only for entertainment and creative purposes but also for malicious activities such as misinformation campaigns, identity theft, reputational harm, financial fraud and political manipulation. These risks are particularly significant in a digitally expanding country like India, where millions of people rely on online platforms for information, communication and public discourse. The rapid spread of manipulated media can therefore undermine public trust, disrupt democratic processes and pose serious threats to individual privacy and security.

The emergence of deepfakes presents new challenges for existing legal and regulatory frameworks. Traditional laws governing defamation, fraud and cybercrime were not specifically designed to address the complexities of AI-generated synthetic media. In India, several legal provisions may potentially apply to the misuse of deepfakes, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. However, the effectiveness of these laws in dealing with rapidly evolving artificial intelligence technologies remains a subject of debate among legal scholars, policymaker and technology experts.

In this context, examining India's legal preparedness to address deepfakes and digital deception has become increasingly important. The absence of specific legislation targeting deepfake technology raises questions about regulatory gaps, enforcement mechanisms and the responsibilities of digital platforms in preventing the spread of manipulated content. Additionally, the cross-border nature of digital media and the speed at which misinformation spreads online further complicate legal enforcement.

This research paper seeks to analyze the problems emerging from the use of deepfakes and digital deception techniques from the Indian perspective. It evaluates the adequacy of existing legal frameworks in addressing the misuse of synthetic media and highlights the challenges faced by lawmakers and enforcement agencies. By examining relevant laws, policy measures and emerging regulatory debates, the study aims to contribute to the ongoing discussion on strengthening India's legal and regulatory response to protect digital integrity, individual rights and public trust in the evolving digital landscape.

DEEPFAKE: CONCEPT AND CHALLENGES IN DIGITAL ERA

Firstly, we have to understand the meaning of the term deepfake in order to know the potential threats caused by this technology. Creating a deepfake itself is not problematic until such deepfakes are used for the purpose of spreading misinformation and other illegal activities by the person making it.

The term deepfake derives from the combination of two words, deep and fake, where 'deep' refers to the *deep learning* while 'fake' generally means something that is not genuine, real or authentic. The deepfake is an artificial image or video or audio generated by a special kind of machine learning called "deep" learning. Deep learning is similar to any kind of machine learning, where an algorithm is fed examples and learns to produce output that resembles the examples it learned from. Humans learn the same way, a baby might try eating random objects and it quickly discovers what is edible and what is not.

Deepfakes are a particularly significant and growing tool for misinformation and digital impersonation. Deepfakes are generated by machine-learning algorithms that can create realistic digital likenesses of

individuals without permission. When execution is excellent, the result can be an extremely believable, but totally fabricated text, video or audio clip of a person doing or saying something that they did not.[1] Deepfakes have the potential to cause significant harm. Nowadays, they have been used to create fake news, false pornographic videos and malicious hoaxes, usually targeting well-known people such as politicians and celebrities. Potentially, deepfakes can be used as a tool for identity theft, extortion, sexual exploitation, reputational damage, ridicule, intimidation and harassment.[2]

Types of Deepfakes

Deepfakes are synthetic media generated using artificial intelligence to manipulate or fabricate audio, images or video content. By leveraging techniques such as machine learning, Generative Adversarial Networks (GANs), and deep neural networks, deepfakes can convincingly alter appearances, voices or movements of real people or create entirely fictional characters. Deepfakes can be broadly classified into several types based on the nature of manipulation which are as follows:

Face Swap Deepfakes: Face swap deepfakes involve replacing the face of one person with another in images or videos while preserving the original body movements and environment. This technique commonly relies on models such as Generative Adversarial Network to produce realistic facial features and expressions. Although widely used in entertainment and digital media editing, face swap deepfakes can also be misused for impersonation, spreading misinformation and creating non-consensual or deceptive visual content.

Face Reenactment (Expression Manipulation): Face reenactment deepfakes manipulate the facial expressions and movements of a person by transferring expressions from a source actor while maintaining the target individual's identity. Technologies such as Face2Face enable realistic modification of facial movements in videos. While useful in animation and visual effects, this technique can also lead to manipulated videos that falsely portray a person's reactions, emotions or speech.

Lip-Sync Deepfakes: Lip-sync deepfakes alter mouth movements in videos so that they match new or modified audio. Artificial intelligence models analyze speech patterns and generate corresponding lip movements to make the altered speech appear natural. Tools like, Wav2Lip are capable of producing highly convincing results. However, such manipulation can make individuals appear to say things they never actually said which potentially leads to spread misinformation or reputational damage.

Entire Face Synthesis: Entire face synthesis refers to the generation of completely artificial human faces that do not correspond to real individuals. These images are produced using generative models such as StyleGAN trained on large datasets of facial images. While this technology is useful for research, gaming and digital avatars, it can also be exploited to create fake identities or deceptive online profiles.

Voice Deepfakes (Audio Deepfakes): Voice deepfakes involve cloning or synthesizing a person's voice using machine learning algorithms trained on audio recordings. Systems like, Tacotron can reproduce speech that closely resembles a specific individual's tone and speaking style. Although voice synthesis is

[1] Northwestern Buffett Institute for Global Affairs, The Rise of Artificial Intelligence and Deepfakes, *available at:* https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf (last visited on March 4, 2026).

[2] eSafety Commissioner, Deepfake Trends and Challenges – Position Statement, *available at:* https://www.esafety.gov.au/sites/default/files/2022-01/Deepfake-position-statement_v2.pdf (last visited on March 4, 2026).

valuable for virtual assistants and accessibility tools, it also raises concerns regarding impersonation, fraud and manipulation of audio evidence.

Synthetic Video (Text-to-Video Deepfakes): Synthetic video deepfakes are created entirely by artificial intelligence without relying on existing footage. These systems generate realistic scenes, characters and movements based on text prompts or instructions. Advanced models such as Sora and Runway Gen-2 demonstrate the capability to produce high quality video content. While this technology has potential applications in media production and storytelling, it also increases the difficulty of verifying the authenticity of digital video content.

Deepfake possesses a challenge for the law makers and law enforcement agencies in prevention of cyber crimes in India. Recent reports show increasing cases involving deepfake technology. Cybercriminal groups in India have used deepfake video calls and manipulated documents to impersonate law-enforcement officials, defrauding victims of large amounts of money. Such scams include "digital arrest scams," voice cloning frauds and fake celebrity endorsements.[3]

DIGITAL DECEPTION: A MUCH BROADER CONCEPT THAN DEEPFAKE

Digital deception is a much broader term than deepfake. When an individual intentionally uses the digital content to deceive another individual or groups then such deception can be termed as digital deception. Deepfake is notably a subset of digital deception as it is one of the forms of digital deception. It can be said that all deepfakes are digital deception, but not all digital deception is a deepfake.

Digital deception refers to the deliberate creation, manipulation or dissemination of digital content with the intention to mislead or manipulate individuals, groups or the public. It exploits the characteristics of digital technologies such as speed, scale, anonymity and accessibility to distort reality, misinform audiences or influence behaviour. Unlike traditional deception, which may occur face-to-face or through print media, digital deception thrives in online environments where content can be easily altered, shared and amplified.

Digital deception encompasses a wide range of phenomena, including but not limited to, the spread of misinformation and disinformation, phishing scams, bot-generated content and AI-manipulated media. Unlike traditional forms of deception, digital deception leverages the speed, reach and anonymity of digital platforms, allowing false or misleading content to spread rapidly and often undetected. This makes it particularly potent in shaping perceptions, opinions and behaviours in both individual and societal contexts.

The consequences of digital deception are profound and multifaceted. At the individual level, exposure to deceptive content can distort perceptions, influence decision-making and erode trust in digital media. On a societal level, widespread digital deception can compromise democratic processes, exacerbate social polarization and facilitate cybercrime and financial fraud. Furthermore, the rapid evolution of digital technologies presents ongoing ethical, legal and regulatory challenges emphasizing the need for comprehensive statutory legal frameworks to mitigate the impact of frauds and illegal activities with use of digital deception techniques.

Case Studies of Digital Deception and Deepfakes in India

[3] TNN, UP STF busts gang behind digital arrest of academic who lost ₹95L; 2 held from Thane, The Times of India, *available at:* https://timesofindia.indiatimes.com/city/lucknow/up-stf-busts-gang-behind-digital-arrest-ofacademic-who-lost-rs95l-2-held-from-thane/articleshow/122940136.cms (last visited on March 5, 2026).

In recent years, many cases relating to the misuse of deepfakes and other forms of digital deception came to light, which include, high-value financial frauds using AI-generated videos to dupe victims of lakhs of rupees, deepfake videos of public figures circulated to mislead and defame, non-consensual explicit content created through AI leading to personal harm and politically sensitive manipulated videos shared online during elections.

Deepfake Investment Scam Using Finance Minister's Identity: Deepfake technology has increasingly been used by cybercriminals to impersonate public figures and promote fraudulent financial schemes. A deepfake video circulated on social media showing Smt. Nirmala Sitharaman, India's Finance Minister, allegedly endorsing an online trading platform. The video appeared authentic and encouraged viewers to invest money in the platform.

A 54 year-old woman from Bengaluru believed the video to be genuine and registered on the platform. She provided personal details and began investing small amounts. The scammers manipulated the interface to display large profits and convinced her to pay additional fees and taxes in order to withdraw the funds. Over a period of three months, she transferred ₹33.25 lakhs across multiple transactions before realizing it was a scam.[4]

Viral Deepfake Video of Actress Rashmika Mandanna: In 2023, a viral video circulated on social media appearing to show Rashmika Mandanna entering an elevator wearing a revealing outfit. The video was later revealed to be a deepfake in which her face was superimposed onto the body of Zara Patel, a British-Indian social media influencer who originally posted the video. The manipulated clip spread widely across social media platforms and triggered public outrage. Authorities registered a case under sections related to forgery, identity theft and privacy violations under the Indian Penal Code, 1860 and the Information Technology Act, 2000.[5]

Political leaders are increasingly becoming targets of AI-generated videos designed to spread misinformation or damage reputations during politically sensitive periods.

Deepfake Video Targeting Punjab Chief Minister Bhagwant Mann: In 2025, a deepfake video circulated on social media showing Shri. Bhagwant Mann, the Chief Minister of Punjab, in an obscene and manipulated video. The clip appeared highly realistic and spread rapidly across online platforms. Punjab Police's cybercrime unit registered a First Information Report (FIR) under relevant sections of the Indian Penal Code and the Information Technology Act for defamation, misuse of technology and spreading misleading content after determining that artificial intelligence tools had been used to generate the video.[6]

The cyber crime cases related to the use of deepfakes and other forms of digital deception are increasing rapidly. The growing advancement of the technology and the easy accessibility of the artificial intelligence (AI) tools among individuals have resulted in potential misuse of the technology in the

[4] "Deepfake of Nirmala Sitharaman costs woman Rs 33 lakh in Bengaluru," The Times of India, December 9, 2025, *available at* https://timesofindia.indiatimes.com/city/bengaluru/deepfake-of-nirmala-sitharaman-costs-woman-rs-33-lakh-in-bengaluru/articleshow/125875466.cms (last visited on March 5, 2026).

[5] Shivani Mankermi, "ETimes Explainer: The Truth Behind Rashmika Mandanna's Deepfake Decoded with Violation of Privacy Rules, Legal Implications and Technological Drawbacks," The Times of India, Nov. 8, 2023, *available at:* https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/etimes-explainer-the-truth-behind-rashmika-mandannas-deepfake-decoded-with-violation-of-privacy-legal-implication-and-technological-drawbacks/articleshow/105070445.cms (last visited on March 5, 2026).

[6] "CM Mann's AI Deepfake Video Sparks FIR, Cops Tracing Creator", The Times of India, Oct. 21, 2025, *available at:* https://timesofindia.indiatimes.com/city/chandigarh/cm-manns-ai-deepfake-video-sparks-fir-cops-tracing-creator/articleshow/124725491.cms (last visited on March 5, 2026).

commission of cyber crimes. Deepfakes are largely used to tarnish the reputation of any individual and spread misinformation which reduces public trust. It becomes difficult for the viewers to ascertain the truth or falsity of any image, audio or video of any person which leads to misinformation, manipulation of public opinion and erosion of trust in digital media. India needs a specifically strict regulatory framework to overcome these challenges possessed by deepfake and digital deception technologies. Now in the next segment, we will understand the existing laws and provisions dealing with the offences related to deepfake and digital deception in India.

EXISTING LEGAL FRAMEWORK RELATED TO DEEPFAKE AND DIGITAL DECEPTION IN INDIA

Although India does not yet have legislation specifically designed to regulate this technology, several existing legal frameworks provide remedies against the misuse of deepfakes. Statutes such as the Information Technology Act, 2000, provisions introduced under the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023 offer mechanisms to address concerns including violations of privacy, reputational damage and the creation and dissemination of obscene or misleading content. However, despite offering some level of protection, these frameworks remain inadequate in fully addressing the evolving challenges posed by generative AI technologies.

The Information Technology Act, 2000 (Act No. 21 of 2000)

The Information Technology Act, 2000 has provided multiple provisions criminalizing deepfake conduct. Some of them are as follows:

- **Section 66C**: This section states that whoever fraudulently or dishonestly uses another person's electronic signature, password or unique identification feature shall be punished with imprisonment of up to three years and a fine of up to one lakh rupees.[7]
- **Section 66D**: This section targets cheating through personation by electronic means. Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.[8]
- **Section 66E**: This section penalizes breaches of privacy, such as capturing or transmitting private images without consent. The use of deepfake technology to exploit personal likenesses without permission can be covered under this provision.[9]
- **Section 67:** This section prohibits the electronic transmission of obscene material. Deepfake pornography, a prudent misuse of this technology falls under the ambit of this section and its punishment.[10]

The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)

The Bharatiya Nyaya Sanhita, 2023 which came into effect from July 1, 2024 has provided certain provisions to deal with offences relating to deepfake and digital deception, some of which are as follows:

[7] The Information Technology Act, 2000 (Act 21 of 2000), s. 66C.
[8] The Information Technology Act, 2000 (Act 21 of 2000), s. 66D.
[9] The Information Technology Act, 2000 (Act 21 of 2000), s. 66E.
[10] The Information Technology Act, 2000 (Act 21 of 2000), s. 67.

- **Section 77 (Voyeurism):** This provision penalizes the capture or dissemination of images of a woman engaged in a private act where she has a reasonable expectation of privacy. The creation or circulation of AI-generated or manipulated images depicting a woman in a private or intimate situation without her consent may constitute an offence under this provision.[11]
- **Section 111 (Organised Crime):** This provision recognizes organised cyber crime involving coordinated deepfake campaigns. It applies when organised networks create and distribute manipulated media for purposes such as misinformation, fraud, blackmail or reputational harm.[12]
- **Section 318 (Cheating):** This provision defines cheating as deceiving a person to induce them to act or deliver property, resulting in harm to body, mind, reputation or property. It may be invoked in cases where deepfakes are used to deceive individuals or cause harm through fraudulent or misleading representations.[13]
- **Section 351 (Criminal Intimidation):** This provision criminalizes acts of intimidation where a person threatens another with injury to cause alarm or compel them to act or refrain from acting. The creation or use of deepfakes to threaten reputational harm or other injury may therefore constitute criminal intimidation under this provision.[14]
- **Section 353 (statements conducing to public mischief):** This provision prescribes three-year imprisonment with fine for statements causing fear or alarm. It also covers statements inciting enmity between groups based on religion, race, birth, residence, language or community. The provision can apply to the dissemination of deepfakes or AI-generated synthetic content that spreads false claims, misinformation or material capable of provoking communal tension or public disorder.[15]
- **Section 356 (Defamation):** This provision defines defamation as the making or publication of any imputation through words, writing, signs or visible representations with the intent to harm a person's reputation. Creating or disseminating manipulated or AI-generated deepfake that falsely portrays an individual and damages their reputation may constitute defamation under this provision.[16]

The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)

The Digital Personal Data Protection (DPDP) Act, 2023 establishes India's framework for protecting personal data, emphasizing consent, purpose limitation and accountability. Biometric data, including facial features, voiceprints and iris scans, is classified as sensitive personal data, requiring explicit consent for processing. Deepfakes leveraging biometric information such as facial recognition extraction, voice cloning or iris-based identity simulation without meaningful consent violate these principles.[17]

Under this Act, major violations involving sensitive data incur penalties up to ₹250 crore, explicitly covering large-scale biometric-based deepfakes. Research implications include legal analysis, ethical evaluation and technical frameworks for consent-based AI use.

[11] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 77.
[12] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 111.
[13] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 318.
[14] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 351.
[15] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 353.
[16] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 356.
[17] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These rules were framed under the Information Technology Act, 2000. It imposes certain obligations on the intermediaries such as social media platforms to regulate harmful digital content. They are particularly relevant for addressing deepfake misuse:

- **Due diligence obligations:** Intermediaries must prevent the hosting or sharing of unlawful content, including defamatory, obscene, misleading or privacy-violating material such as harmful deepfakes.
- **Takedown mechanism:** Platforms are required to remove or disable access to unlawful content within a prescribed time frame upon receiving a valid complaint or government order.
- **Grievance redressal system:** Intermediaries must appoint a Grievance Officer to address user complaints related to harmful digital content, including manipulated or AI-generated media.
- **Additional compliance for significant social media intermediaries:** Appointment of a Chief Compliance Officer, Nodal Contact Person and Resident Grievance Officer ensures accountability.
- **Cooperation with law enforcement:** Platforms must preserve information and assist authorities in investigations involving illegal content, such as deepfake-based harassment, defamation or misinformation.

While these rules provide procedural remedies for removing harmful content, they do not specifically define or regulate deepfakes or generative AI, highlighting the need for more targeted AI-specific legal frameworks.

JUDICIAL RESPONSE ON DEEPFAKE AND DIGITAL DECEPTION IN INDIA

In the case of ***Anil Kapoor* v. *Simply Life India & Ors.,***[18] actor Anil Kapoor filed a suit before the Delhi High Court against the unauthorized use of his name, image, voice and persona on digital platforms, including AI-generated content. The Court granted an interim injunction restraining the defendants from exploiting his personality attributes without consent. It recognized that technologies such as AI and deepfakes can replicate a person's likeness and voice. The Court held that such acts violate personality rights and the right to publicity. The judgment directed the removal of infringing online content. It is an important precedent addressing AI-based impersonation in India.

In ***Mr. Akira Desai alias Akira Nandan v. Sambhawaami Studios LLP & Ors.,***[19] Akira Nandan filed a case against unauthorized AI-generated use of his likeness and persona. The Delhi High Court granted an injunction restraining the defendants from using or distributing the content. The Court recognized that AI and deepfakes can harm reputation and violate personality rights and privacy under Article 21 (Right to Life and Personal Liberty) and Article 19(1)(a) (Freedom of Speech) of the Constitution of India. This case highlights judicial recognition of digital impersonation issues in India.

In the case of ***National Stock Exchange of India Ltd. v. Meta Platforms, Inc. & Ors.,***[20] the Bombay High Court ordered meta (facebook and whatsApp) to remove a deepfake video of NSE chairman Ashish Kumar Chauhan which were misleading investors with false stock tips and urging them to join scam WhatsApp groups.

[18] CS (COMM) 652/2023 (Del HC).
[19] CS(COMM) 68/2026 (Del HC).
[20] IA (L) No. 21456 of 2024 (Bom HC).

In ***Karan Johar v. Ashok Kumar/John Doe & Ors.,***[21] the Delhi High Court granted an interim injunction protecting the plaintiff's personality and publicity rights. The Court held that unauthorized use of his name, image, voice, likeness and AI-generated content by the defendants caused irreparable reputational harm and misleading public perception. Offensive or disparaging content was not protected under fair use or satire. Defendants were directed to remove infringing material, highlighting the Court's recognition of the growing threat of AI and deepfakes to celebrity rights.

CONCLUSION AND SUGGESTIONS

The rise of deepfake technology and other forms of digital deceptions represents a profound challenge to personal privacy, social trust and the integrity of democratic processes in India. As this study demonstrates, while India has a growing body of cyber laws, including provisions under the Information Technology Act, 2000 and relevant sections of the Bhartiya Nyaya Sanhita, 2023, these legal frameworks are largely reactive and not specifically designed to address the unique threats posed by deepfakes and digital deception. The technology's ability to manipulate audio-visual content with high fidelity has outpaced the current regulatory and judicial mechanisms, leaving gaps in prevention, detection and accountability.

Despite the rapid proliferation of deepfakes, India currently lacks comprehensive legal, technological and regulatory mechanisms to effectively detect and deter such digital manipulations. Addressing this gap through strengthened laws, AI-driven detection systems, public awareness initiatives and international collaboration is crucial not only to safeguard individual rights and reputations but also to protect national security, democratic processes and the integrity of public discourse.

After a detailed discussion on the challenges of deepfake and digital deception technologies, my suggestions are that India must adopt a multi-pronged approach to effectively combat the challenges posed by deepfakes and other forms of digital deceptions.

Firstly, the legal framework should be strengthened by amending the Information Technology Act, 2000 and introducing dedicated legislation that explicitly criminalizes the creation, distribution and misuse of deepfake content, drawing on international models such as the U.S. Deepfakes Accountability Act (a Bill introduced on 20/09/2023 in U.S. Congress to protect national security against the threats posed by deepfake technology and to provide legal recourse to victims of harmful deepfakes which was subsequently referred to the Subcommittee on Emergency Management and Technology).

Secondly, a dedicated regulatory authority under CERT-In or the Ministry of Electronics and IT (MeitY) should be established to monitor malicious digital content and coordinate swift legal action.

Thirdly, technological solutions including AI-powered detection tools, digital watermarking and blockchain-based verification systems should be promoted to ensure the authenticity of digital media.

Fourthly, public awareness campaigns and the integration of media and digital literacy into educational curriculum are essential to empower citizens to recognize manipulated content and misinformation.

Fifthly, active collaboration with technology companies, startups and social media platforms is critical for developing detection tools, enforcing content moderation and providing efficient reporting mechanisms.

Sixthly, international cooperation through bilateral and multilateral agreements, knowledge sharing with global cybercrime units and cross-border enforcement strategies will enhance India's ability to address the transnational nature of deepfake threats.

[21] CS(COMM) 974/2025 (Del HC).

Together, these measures can provide a comprehensive legal, technological and social framework to mitigate the risks posed by deepfakes and digital deception in India.

REFERENCES

1. Anil Kapoor v. Simply Life India & Ors., CS (COMM) 652/2023 (Del HC).
2. Karan Johar v. Ashok Kumar/John Doe & Ors., CS(COMM) 974/2025 (Del HC).
3. Mr. Akira Desai alias Akira Nandan v. Sambhawaami Studios LLP & Ors., CS(COMM) 68/2026 (Del HC).
4. National Stock Exchange of India Ltd. v. Meta Platforms, Inc. & Ors., IA (L) No. 21456 of 2024 (Bom HC).
5. The Constitution of India, 1950.
6. The Information Technology Act, 2000 (Act No. 21 of 2000).
7. The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).
8. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
9. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
10. www.buffett.northwestern.edu
11. www.esafety.gov.au
12. www.timesofindia.indiatimes.com