Journal of Law and Legal Research Development
ISSN: 3048-5045

Deepfake Crimes in India: Rethinking Cybercrime Regulation and Criminal Liability

Bhagavathy V*

Student, LL.M. (Cyber Law), School of Law, Joy University, Vadakankulam, Tirunelveli, Tamil Nadu, India

Review Article History

Received: 20-Jul-2026
Revised: 25-Jul-2026
Accepted: 27-Jul-2026
Published: 31-Jul-2026

Keywords

Artificial Intelligence
Criminal Liability
Cybercrimes
Deepfakes
Intermediary Liability
Privacy
Synthetic Media

Abstract

The fast-paced technological progress in the realm of artificial intelligence and generative technologies has changed the way content is being created and edited in the digital sphere. One of the major outcomes of such technological advancement is the appearance of deepfakes – technology capable of manipulating a person's face, voice, facial expressions or behaviour to produce fictional audio-visual content. While there is certainly a place for synthetic media in the realms of entertainment, educational purposes, and accessibility, as well as within creative industries, its misuse has led to the emergence of serious legal challenges related to identity theft, fraud, sexual exploitation, defamation, violation of privacy, damage to reputation and disinformation. Traditionally, in India, such actions were punished using technology-neutral laws of the Information Technology Act 2000, the Indian Penal Code and more recently the Bharatiya Nyaya Sanhita 2023, along with intermediary regulation according to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Significant changes in the regulatory framework have happened due to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 regulating synthetically generated information and imposing new due diligence responsibilities on intermediaries. However, challenges persist on the aspects of attribution, mens rea, evidential reliability, liability of intermediaries, enforcement across borders and the difference between harmful misrepresentations and constitutionally protected speech. In this paper, the response to crimes by deepfake technology in India's evolving law will be assessed critically and a framework proposed, which includes technology neutral criminal offenses together with procedural and evidential procedures and governance of the platforms instead of developing an overly expansive standalone offense.

Corresponding Author:
Bhagavathy V *
Student, LL.M. (Cyber Law), School of Law, Joy University, Vadakankulam, Tirunelveli, Tamil Nadu, India
bhagavathy561@gmail.com

1. INTRODUCTION

Artificial intelligence (AI) has revolutionized the way digital communication takes place by creating opportunities to make images, audio, and video look like something realistic which was previously very challenging to produce. One of the most important advancements in this sphere would be deepfakes. A deepfake might be described as an artificial audio-visual representation made or edited by artificial intelligence or similar technology that makes a person appear to be saying or doing things that are false. The possibility to reproduce somebody's face, voice, behaviour and facial expression is useful for many different purposes, but at the same time, it gives rise to the possibilities of fraud, impersonation, etc. The problem from the legal point of view is that deepfake technology is not illegal per se. In other words, the same technology could be used to make harmless content or even art, or it could be used for fraud, sexual exploitation of someone else's image, impersonation and so on. The key thing here is not the fact that some synthetic content has been created, but rather its illegality, intention and effect on third parties. It has

become especially relevant for India as social media platforms allow synthetic content to be accessed by millions of people in a very short span of time. Fabricated content about a public person may have already been spread for thousands of times by the time that the individual becomes aware of such content being generated about himself or herself. In other words, the damage is not just restricted to the creation of such material. Uploading, forwarding, posting and algorithmic propagation may turn an act of manipulation into a social issue. In Indian criminal laws, the approach towards cybercrimes has been technology neutral. Provisions dealing with identity theft, cheating by personation, privacy violation and sexually explicit material are contained in the Information Technology Act, 2000. Cheating, forgery, defamation and public mischief are dealt with in the general criminal laws. Enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS) has made the Indian Penal Code redundant and brought in the current criminal laws. Section 319 of the BNS recognizes cheating by personation while there are provisions for forgery, electronic record, public mischief and defamation (Bharatiya Nyaya Sanhita, 2023). The regulatory landscape has once again undergone a transformation. On 10 February 2026, the Ministry of Electronics and Information Technology issued amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The amendments incorporated the notion of "synthetically generated information" and specifically made the same kind of information subject to the due diligence process under the intermediary. The amendments took effect from 20 February 2026. This framework is notable since it goes beyond the use of generic terms such as "unlawful online information." It acknowledges that the audio-visual information which has been created synthetically could imitate a person or an actual event in a manner that it is perceived as being identical to real-life events. It imposes obligations regarding the unlawful synthetic content, labelling, metadata, and technical measures, among others. The primary thesis of this paper is that the Indian law should not rely solely on the creation of a specific offence known as “deepfake crime.” The abuse of deepfakes may assume numerous forms, and one type of offence may be too narrow to cover any future technological developments or too wide to identify any illegal activity. Rather, what India needs is an overarching model where existing criminal offences would be used depending on the level of harm caused, and particular regulations regarding synthetic media will facilitate prevention, detection, traceability and platform accountability.

2. DEEPFAKES TECHNOLOGY AND CRIMINALISATION OF SYNTHETIC DECEPTION

Deepfake technology is usually understood as face swapping, voice impersonation, and video manipulation. However, the more general notion of the use of such technology implies a number of varieties of synthetic media. One’s face may be added to someone else’s body, a person’s voice may be recreated using artificial technology, facial movements may be created to match fake speech, or an entire fake scene might be created to represent the participation of an individual in an incident that did not happen. What is crucial in the legal perspective here is not the manipulation itself but the generation of false images. It has been established that synthetic media impacts the reliability of digital communication in that people start to rely on visual and audio data as evidence of events. Chesney and Citron (2019) pointed out that there are additional risks related to deepfake in that these risks are not limited to individuals but can affect democratic institutions and public dialogue as well. Westerlund (2019) also considered such aspects as misinformation, fraud, political manipulation, and reputation damage as the main risks involved in deepfake use. The scalability is another feature of deepfakes. In order to falsify a picture or an audio file, one had to possess some skills. Artificial intelligence has removed this requirement. Now, an average user might be capable of producing a deepfake with a much smaller set of technical skills than before. Thus, there is a legal risk as well since there are significantly more offenders than before. One more feature to consider is speed. If fake content is put online on a social media site, it can be copied and distributed without any further involvement of the original author. Deletion of the initial copy will not necessarily take it off the internet since there can be copies of it available on different websites, social media platforms, messengers and even in private communities. This is another difference between the offenses which are based on traditional publication and modern threats of the digital world. Deepfakes may be associated with something called “authenticity crisis.” In case the falsified information is convincing enough, people may question the authenticity of real-life records. It is one more aspect of the so-called “liar's dividend,” as mentioned above. Accused people may discredit real life records by referring to the technology of their creation using artificial intelligence (Chesney & Citron, 2019). So deepfake videos are able to harm even in cases when no one really believes in them. The criminal law needs to differentiate between synthetic media as a technological tool and the misconduct which is the subject matter of regulation. A fictional movie using the image of the performer with his or her consent is completely different from the synthetic video made to dupe the victims and make them part with their money. Similarly, the educational simulation of a fictional nature cannot be automatically regarded as equivalent to a synthetic video which deceives its viewers. The correct question would therefore be “Is an unlawful act committed through the use of AI?” The key idea here is to ensure the development of technology without any abuse.

3. INDIAN LEGAL FRAMEWORK

India does not have one statute for deepfake regulation. The Indian legal system provides for the overlapping cyber law, criminal law, intermediary law, privacy and torts. The IT Act, 2000 continues to form the core of the cybercrime law. Sections 66C and 66D are applicable where deepfakes are being used for identity theft or cheating by personation. Section 66E covers cases of violation of privacy. Section 67 and 67A may become applicable where obscene or sexual synthetic material is at issue. The significance of the IT Act is due to its applicability to conduct concerning computer resources and electronic communications. Nonetheless, the Act was passed way back in 2000, before the emergence of contemporary generative artificial intelligence. Therefore, it lacks terminology pertaining to deepfakes. This doesn't automatically mean that it cannot be applied to deepfake-related crimes, seeing as there are certain provisions in the Act that are technologically neutral. However, the lack of terminology specifically addressing synthetic identity impersonation may pose interpretation issues in novel circumstances. The BNS forms an additional basis in the criminal law applicable to deepfakes. Section 318 deals with cheating, whereas Section 319 covers the crime of cheating by personation and offers punishment for someone pretending to be someone else or making out someone else as some other

person. This section is especially pertinent to deepfake cheating cases as synthetic voice or video can form a pretend identity and lead the deceived party into action. Moreover, BNS also includes provisions with respect to forgery, making false documents, forgery of electronic records, and the use of forged electronic records as authentic. Therefore, Sections 335, 336, and 340 might apply to the cases where synthetic material is included in a false electronic record or fraudulent act. Not all deepfake videos would amount to forgery. In such a case, it is the responsibility of the prosecution to prove the elements of the crime. Under Section 356 of the BNS, defamation law may come into effect when false imputations against someone are made through synthetic materials and damage their reputation. One significant point about the Indian legal system with regard to the issue at hand is that deepfake videos do not constitute any independent kind of damage just because AI technology was involved. IT Rules have become more and more relevant due to the fact that they are regulating the activities of the intermediaries. Thus, the amendments made in 2026 can be considered as one of the most notable because synthetically generated information was defined. According to the new amendments, synthetically generated information means audio, video or audio-visual information that was artificially or algorithmically produced, generated, modified or edited with the help of a computer resource in such a way that it seems to be true and represents a person or an event in a manner that would be considered indistinguishable from reality. This provision has legal relevance because without this exception regular editing, colour correction, transcribing and making materials accessible for the disabled people may be covered by too broad a definition of synthetically generated information. These amendments also require that the intermediaries which help create or publish synthetic information should take reasonable technical steps to prevent the illegal use of synthetic information. Child sexual abuse material, non-consensual intimate images, obscene or sexually explicit information, false electronic document, and synthetic information which misrepresents the identity, behaviour, statement, or an actual incident to deceive are considered prohibited categories. Legal synthetic information shall be marked in a prominent way, and where technically possible, there should be permanent metadata or some other provenance mechanisms to mark the synthetic information. There are certain additional obligations for significant social media intermediaries, including requiring that users state whether information is synthetic or not, and also taking technical measures to verify such statements. If synthetic information is discovered, it needs to be prominently labelled. The proposed amendments therefore constitute a move away from a purely reactive method to a combination of preventive and traceability measures. Nevertheless, regulation of the intermediary does not equate to criminal liability. A platform's non-compliance with its due diligence obligation is a legal situation distinct from that of the criminal liability of an individual for intentionally producing a deepfake. The distinction is necessary so as to not subject platforms to automatic criminal liability for each illegal message generated by users. The Digital Personal Data Protection Act of 2023 is also a component of the broader privacy framework. The Act acknowledges the protection of digital personal data while allowing processing of personal data for permissible purposes. The production of deepfakes entails the unauthorized use of photographs, biometric features, voice recordings or personal data. Therefore, data protection regulations could serve as complementary to criminal laws even though data protection law cannot replace criminal law entirely.

4. CRIMINAL LIABILITY AND ATTRIBUTION

The most vexed issue in deepfake criminal law is that of criminal attribution. A typical deepfake case could include one individual who has collected pictures of the victim, another individual who has made the deepfake material, a third individual who has added fraudulent text to it, someone who has uploaded the video, thousands of individuals who knowingly share it and the platform hosting it. To make everyone criminally liable on the same level would be contrary to some of the fundamentals of criminal law. Ordinarily, criminal liability should depend upon actions, knowledge and intention of an individual. An individual who has intentionally created a fake video to deceive another is fundamentally different from an individual who has unwittingly shared a video thinking that it is genuine. Also, someone who has received a fake video, known it to be fake and distributed it to tarnish the reputation of an individual is more guilty than an individual sharing the video without knowing its fraudulent nature. The mens rea element is, therefore, crucial. The criminalization of deepfakes would mean that any technological creation would constitute a crime, simply because somebody somewhere dislikes what the person who created it has done. Criminalizing the making of such an image or video, when it is clear that it is fiction and labelled as synthetic, would be a wrong decision if the creator had no intention or knowledge that his creation could be considered offensive to some other person. One of the areas in which criminal liability may arise due to deepfakes is fraud. For example, a voice of a deepfake which resembles that of a bank employee, a company executive or a family member can be used to convince victims to transfer money. When the deception is coupled with dishonest inducement and loss, there are cheating and personation laws that can support prosecution. In particular, section 319 of the BNS is pertinent in that it deals explicitly with the impersonation. Sexual abuse through the use of deepfakes is another form of injury that is distinct. Violations of privacy and dignity may occur in cases where there is any non-consensual intimate imagery. In 2026 IT Rules, both non-consensual intimate imagery and sexually explicit synthetic content have been specified as offenses against which intermediaries need to deploy preventive actions. In case the victim is a minor, then an offense could be created according to the Protection of Children from Sexual Offences Act, 2012. The use of defamatory deepfakes creates another problem. The injury is not necessarily caused by any monetary loss. A fake video showing an individual making any obscene, immoral or criminal statement may affect employment and professional reputation. Therefore, defamation laws could be pertinent here. The issue is that with digital transmission, injury can be much greater in scope as compared to traditional publication due to repeated access to the material. The intermediary liability issue needs to be considered separately. In India, there is conditional safe-harbour under Section 79 of the IT Act. According to the 2026 Rules, removal or disabling access to the synthetic information in accordance with the Rules does not per se violate the conditions for safe harbour. This is important since the platform must have legal certainty in order to remove synthetic information without facing potential liability for doing so. Nevertheless, safe harbour cannot mean exemption from all responsibilities. According to the 2026 Rules, significant social media intermediaries must conduct technical verification and labelling of synthetic information. Therefore, the right way would be to create a system of conditional responsibility: platforms must not be viewed as the original actors of any offences committed by

their users, but they have to undertake defined legal due diligence upon identification of certain risks or unlawful information.

5. CONSTITUTIONAL AND JUDICIAL ASPECTS

Any regulation concerning Deepfake videos should not contravene the Constitution. The right to freedom of speech and expression is protected under Article 19(1)(a) of the Constitution. Additionally, Article 21 has been held to cover the right to privacy and dignity among others. The regulation would therefore be a balance of two constitutional values and not a restriction of synthetic media. There is the danger that a total ban on any sort of manipulated or AI-generated content will have a negative impact on legitimate speech. Political satire, parody, artistic reworking, movie-making, teaching through simulation and commenting might at times require manipulation and AI. This means that regulation that bans every real manipulation will affect legitimate expression.

The constitutional problem becomes worse when there is the need for determination as to whether the content is "false," "misleading," or "deceptive." Determining whether the content is false involving context analysis in some cases. For example, satirical movies might be false when viewed separately but not when considered in the context of the whole program. This means that the mechanism of enforcing the regulation should consider objective categories of illegal content and deception. On the other hand, freedom of expression does not offer unlimited protection for deliberate fraud, impersonation, sexual abuse, or malicious defamation. As noted by the Supreme Court while recognizing privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), it is a foundational constitutional right that ensures individuals against any exploitation from misuse of their personal details and identities. Deepfake legislation will be valid to the extent that it protects privacy and dignity through proportionate measures. Deepfakes are being dealt with by Indian courts under personality and publicity rights. For instance, in Ravi Shankar v. John Doe(s) (2025), the Delhi High Court was dealing with the issue of the creation of fake videos based on the plaintiff's name, voice, facial expressions, persona and likeness. Notably, the importance of the case goes beyond the issue at hand. It shows that the Indian courts are prepared to take artificial intelligence impersonation seriously as a matter of interference with one's personality and publicity rights. The court also ordered the respective platform to delete or block access to the identified infringement during the stipulated time frame. In a similar vein, the Delhi High Court ruled on the issue of AI-generated deepfakes in Aishwarya Rai Bachchan v. Aishwaryaworld.com & Ors. (2025). The Court ordered the defendants not to use her persona using artificial intelligence, machine learning, deepfakes, and face morphing technologies. It also issued directions for the deletion of identified URLs and providing subscriber details. The development of such cases is significant since the criminal law is not the only way of addressing the issues associated with deepfake harms. While the issuance of civil injunction may prove quicker than a criminal action especially when the need is to delete the harmful content, it is worth noting that criminal law remains applicable in situations involving fraud, sexual exploitation, identity theft, etc. This is another illustration of the significance of personality rights in the context of deepfake videos. The voice, face, and mannerisms of an individual may be taken to constitute aspects of personality. Thus, the unauthorized synthetic creation can lead to harm irrespective of whether there has been any copyright violation at all. It appears from the case law that courts in India have adopted certain existing principles rather than awaiting a comprehensive statute for deepfakes.

6. PROBLEMS OF EVIDENCE AND ENFORCEABILITY

A law being in place will not automatically result in successful prosecution. There are evidentiary hurdles associated with deepfakes since it is difficult to trace back the source of the content in question, which may be created on one device and then uploaded from another, possibly through foreign servers and re-uploaded by various people. As such, attributing is a challenge. For example, proving that a particular person made the deepfake entails more than showing that the person had the file created. Investigators have to provide metadata, device data, account information, IP addresses, financial information, communication information, and other evidence. In cases where a synthetic file is found in the device of the suspect, the prosecution has to prove the connection between the defendant and the criminal act. With the improvement of deepfakes technology, courts will find themselves dealing with arguments about whether or not the audio or video evidence has been doctored. As such, digital forensic labs will require efficient detection methods. The issue with detection technologies is that they are not always accurate. A forensic conclusion is better confirmed by using multiple types of evidence. The current law relating to evidence in India is the Bharatiya Sakshya Adhiniyam, 2023. With the increasing use of synthetic media, preservation and authentication of electronic evidence become critical. Investigators must preserve original files, metadata if available, device information and chain of custody. Screenshots alone will not provide the history of the entire digital content. Another issue which arises due to this crime is the issue of cross-border jurisdiction. Some large-scale platforms may have their operations from entities based outside India, while the perpetrator could be based outside the jurisdiction of India. Volume is yet another issue that needs to be considered practically. The police cannot conduct manual investigations into all the manipulated images or videos found on the Internet. Thus, it is essential to apply a risk-based enforcement approach, giving preference to content related to financial fraud, sexual exploitation, threats, elections manipulation, and significant damage to reputation compared to harmless synthetic entertainment. Victim reporting is one more issue. Victims of deepfake sexual abuse might refrain from reporting this to the police due to shame and other reasons. Thus, enforcement requires confidential ways of reporting and fast evidence collection and handling.

7. RETHINKING INDIA'S REGULATORY APPROACH

Indian 2026 synthetic media regulations constitute a great step forward regarding regulation but their success depends on implementation. Regulations have progressed to include the issues of labelling, provenance, verification and platform accountability. Such regulations decrease deception, but do not eliminate malicious deepfakes completely. First, the use of labelling alone is inadequate in India. The usefulness of labelling the content as artificial is dependent upon users noticing it and understanding its significance. An advanced malicious user may try to manipulate content by removing its metadata or reproducing it off-platform. Hence, both the systems of provenance and detection should exist along with processes for reporting and removal. Secondly, criminal liability must continue to be based on harm. A separate offense

of a deepfake might look appealing since it would be statutory and hence clear-cut. However, deepfakes may be used in many criminal activities. Defining one offense may lead to overlap with cheating, identity frauds, privacy violation, sexual offenses, forgery and defamation. It is better to define through statutory guidelines how existing offenses would apply if synthetic technology was involved. Thirdly, Indian law should differentiate participants. The main creator, person who asked for its creation, person who knows about it and disseminates it intentionally, person who distributes it without any knowledge and platform which fails to meet the requirements of the law in some respects must not all be treated the same under criminal law. The fourth issue is that mens rea must be adequately safeguarded. The law should distinguish between the malicious synthetic manipulation and parody, satire, art, education and legitimate research. Thus, victims must have available processes for prompt removal of the material, preservation of evidence and revealing identity of unknown perpetrators. Special courts' practices must be further developed. The sixth problem is the need for law-enforcement training. Police officers, prosecution authorities and judges must have basic knowledge about synthetic media technologies, digital evidence and limitations on the forensics. Otherwise, all the best legislation will be useless. Seventhly, India ought to consider technical provenance requirements. Ideally, such a system ought to be platform-independent rather than relying on a proprietary standard. Cooperation with other countries would make such a system more effective as deepfakes transcend international borders. Finally, there is need for technological neutrality in regulatory legislation. The technologies used to create deepfakes change rapidly. Legislation that specifies a certain software application or way of creating deepfakes may be obsolete in a few years' time. It would therefore be better to regulate harm rather than trying to regulate technology itself.

8. CONCLUSION

The advent of deepfake technology has impacted the nature of digital identity and evidence in a unique way where the face, voice and actions of an individual could easily be simulated, leading to the possibility of committing fraud, sexual abuse, impersonation, defamation and disinformation. The problem that arises out of the issue cannot merely be considered a technological one but rather a case of criminal liability, individual rights, platform regulation and evidentiary problems. The Bharatiya Nyaya Sanhita, 2023 has provisions against the offenses of cheating, personation, forgery, false electronic records, public mischief and defamation. However, the key change has been made to the IT Rules in 2026 that explicitly acknowledged the existence of the artificially created content and brought in certain requirements in relation to unlawful synthetic content and labelling, source of such information and technical verifiability. Regulation, however, does not mean criminalization as the artificial content itself is not necessarily malicious and criminal law should distinguish the two. Judicial changes in India suggest that the courts are already applying the existing concepts of personality, publicity, privacy and remedies against the harms caused by AI technologies. The case involving Ravi Shankar and Aishwarya Rai Bachchan shows the courts' readiness to protect the name, image, voice, likeness, and persona. The future of deepfake legislation in India must therefore lie in an integrative, rather than a duplicating, strategy. India may not necessarily require a broad criminal offence which encompasses every possible type of deepfake. It needs a cohesive regime that comprises of criminal offences already in place, obligations of specialized intermediaries, forensic capabilities, victim recourse, international collaboration and constitutional guarantees. Ultimately, the aim should not be regulating artificial intelligence because it is artificial. It must be in preventing technology from being used as a tool of deception, exploitation and abuse of individual rights. Such a balanced strategy of fostering technological development but at the same time subjecting malicious and artificial deception to repercussions will constitute a better platform for India's AI driven world.

Conflict of Interest
Conflict of interest declared none.

Funding
The review presented in the article did not receive any external financial support.

9. REFERENCES

- Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament, 2023.
- Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, Acts of Parliament, 2023.
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820.
- Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war. Foreign Affairs, 98(1), 147–155.
- Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023.
- Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, G.S.R. 139(E) (2021).
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Gazette of India, G.S.R. 120(E) (2026).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Paris, B., & Donovan, J. (2019). Deepfakes and cheap fakes: The manipulation of audio and visual evidence. Data & Society Research Institute.
- Ravi Shankar v. John Doe(s)/Ashok Kumar(s) & Ors., CS(COMM) 889/2025 (Delhi High Court, Aug. 26, 2025).
- Aishwarya Rai Bachchan v. Aishwaryaworld.com & Ors., CS(COMM) 956/2025 (Delhi High Court, Sept. 9, 2025).
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception and uncertainty. Social Media + Society, 6(1), 1–13.
- Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52.