
DEEPPAKES AND CRIMINAL LIABILITY: AN EXAMINATION OF INDIA'S STATUTORY AND JUDICIAL RESPONSE TO SYNTHETIC MEDIA

Garima Choudhary, Assistant Professor, Department of Law, Gitarattan International
Business School (GIBS), Rohini, Delhi, India

Post Graduate Diploma in Management (PGDM), Amarapali Zodiac, Noida, U.P., India

ORCID: 0009-0006-7252-3267

ABSTRACT

With the advent of generative artificial intelligence, anyone with a bit of technical expertise can now create convincing fake audio, images and video that impersonate a real person as saying or doing something he or she never said or did. Already in India, non-consensual intimate images of women are created; financial frauds are made using their voices; public figures are maligned, and political disinformation is disseminated before elections. This article explores the capabilities of the current Indian criminal law regime, which consists predominantly of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023 and 2026, in the context of synthetic media harms. It explores how the concept of a "deep fake" is being applied to existing offences of forgery, cheating by personation, defamation, criminal intimidation, obscenity and voyeurism and considers the developing judicial doctrine of "personality rights" established by the Delhi High Court. Although the current state of laws and policies provides valuable but incomplete avenues for redress, the focus of the current patchwork of provisions is on the distribution of content and does not specifically target the technology itself; mens rea remains a grey area, and the distribution of synthetic media is cross-border in nature, meaning there are gaps in enforcement. It ends with a proposed calibrated approach to the legislation that aims to stifle the undue use of generative AI without creating undue restrictions on its legitimate use, like satire, art, and research.

Keywords: Deepfakes, Synthetic Media, Criminal Liability, Bharatiya Nyaya Sanhita, Information Technology Act, Personality Rights, Artificial Intelligence, Non-Consensual Intimate Imagery.

I. INTRODUCTION

A video in which the actress Rashmika Mandanna walked into an elevator in a revealing outfits went viral on Indian social media in November 2023 before it became known that her face was digitally superimposed on the body of a British-Indian influencer. The incident had led to a first information report (FIR) being filed by the Delhi Police under the provisions of the erstwhile Indian Penal Code and the information technology forgery and privacy provisions of the Information Technology Act, 2000, that had made a threat that had remained mostly theoretical for Indian policymakers real. The Union Ministry of Electronics and Information Technology issued an advisory to social media platforms reminding them of their due-diligence obligations and cautioning against the use of malicious synthetic media, which has since been renamed "synthetically generated information" in the wake of the incident and warned that such media would be punishable as per law. Deepfakes are media, most often video, audio or still images, created or altered via deep-learning image, video or speech synthesis methods, usually with the help of generative adversarial networks or diffusion models, that are designed to depict a person performing or uttering an act that it is not actually engaged in or that did not happen. While the technology of creating deepfakes is based on real data, unlike previous instances of digital manipulation like Photoshop alterations or video splicing, the machinery to create such forgeries has now become affordable and readily available. The potential harms caused by this technology are not unprecedented in nature, as other technologies have caused harms known to Indian criminal law for a long time, including impersonation, defamation, sexual exploitation and fraud, but the scale, realism and speed of dissemination made possible by generative artificial intelligence are qualitatively new and the capacity of a criminal law that was drafted in time of physical documents and analogue impersonation is being put to the test. This article will be continued in five parts. Part II places the harms caused by deepfake technology in a taxonomy of criminal acts. Part III will analyse the current framework provided by the laws and regulations in India to prosecute and regulate Deepfakes under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Information Technology Rules and their subsequent amendments. Amendments, and allied legislation including the Digital Personal Data Protection Act, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. Part IV surveys the judicial response, with particular attention to the personality-rights jurisprudence developed by the Delhi High Court. Part V identifies the principal doctrinal and enforcement gaps that persist notwithstanding this statutory and judicial activity, and Part VI offers recommendations for reform.

II. DEEPFAKES AS CRIMINAL CONDUCT: A TAXONOMY OF HARM

It is important to first break down the term “deepfakes” into the various types of harms they can entail before analysing the relevant law, because Indian criminal law does not consider synthetic media as a single entity but rather each harm through the lens of the wrong committed.

A1. Non-Consensual Intimate Imagery and/or Sexual Exploitation

The most widely reported deepfake application in India and across the world is creating pornographic videos and images of women without their consent; a common practice includes using the face of a woman who is not being sexually intimate with somebody else in the pornographic content. This behaviour reflects the victim's dignity, privacy and bodily autonomy, even though no physical action has been taken, and disproportionately affects women in public roles, such as actors, journalists and politicians.

A.2. Avoiding Impersonation, Identity Fraud, and Financial Crimes

Voice-cloning and Face-Swapping technology have been employed to mimic corporate executives, family members, and government officials to trick victims into transferring money — a modern twist on the confidence game, also known as “vishing,” which is done over the phone. Unlike the previous email-based phishing, the created voice or video is in many cases, indistinguishable from the authentic one, which makes this fraud even more effective.

A.3. Defamation and Reputational Harm

When a person is shown (deepfaked) saying something they never said, doing something they did not do, or doing a completely different thing, this can cause significant damage to his or her reputation, especially when it is widely shared before the fake is identified and rectified. Public figures, whether they be film stars, journalists, or politicians, have been particularly vulnerable as they have been more easily accessible as a source of training data, and content about them has received more viral distribution.

A.4. Political Disinformation and Electoral Integrity

Synthetic media depicting political candidates making inflammatory or false statements poses a distinct threat to electoral integrity, particularly where such content is disseminated in the closing days of a campaign when there is little time for correction. The Election Commission

of India has cautioned political parties against the use of deepfakes in campaign material, treating such use as a violation of the Model Code of Conduct.¹

A.5. Forgery of Electronic Records and Evidentiary Fabrication

A related, though lesser-known, category of harm is when someone creates a fake recording of audio or video to use as evidence, or when they claim that real evidence is a "deepfake" (a term sometimes known as the "liar's dividend"). Both options challenge the trustworthiness of electronic evidence in judicial trials and present separate legal challenges, which are explored in Part III.

III. THE STATUTORY FRAMEWORK IN INDIA

There is no specific legislation in India against the creation and distribution of deepfakes. In contrast, the prosecution of deepfakes comes from a variety of general and special criminal law provisions in the Bharatiya Nyaya Sanhita, 2023 ("BNS"), which replaced the Indian Penal Code, 1860 from 1 July 2024, and the Information Technology Act, 2000 ("IT Act") along with a growing network of subsidiary rules in the form of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and its subsequent amendments. Each is discussed separately in this part.

A. The Information Technology Act, 2000

The provisions most directly relevant to computer-generated impersonation contained in the IT Act. The offence of section 66C is the fraudulent or dishonest use of another person's electronic signature, password or other identifiers unique to a person, and carries a punishment of imprisonment for up to three years or a fine. Cheating by impersonation by using a computer resource is punished by imprisonment to three years, in the same way as section 66D. Section 66E of the body of privacy protection law under the Protection of Privacy Act is often cited in cases of fabricated intimate imagery and has the potential to criminalise the intentional capture, publication or transmission of an image of a person's private area where the circumstances are intrusive to their privacy. Section 67, penalises the publication or transmission of obscene material and Section 67A penalises the publication or transmission of sexually explicit material

¹Jurigram, Deepfake AI Laws in India: Punishment and Precedent (2026), <https://jurigram.com/blog/cyber-law/deepfake-ai-laws-india-punishment>.

in electronic form, where a second conviction will result in increased punishment. The provisions were intended to cover the traditional types of cybercrime, including the theft of passwords, the dissemination of pre-existing intimate images without consent, and computer-based impersonation for financial fraud — but not when used to create synthetic images, rather than copies or ‘alterations’ of an authentic image, via a machine-learning model. They were written to apply to conventional cybercrime, such as stealing passwords, sharing pre-existing intimate images without the owner's permission, and impersonating a person for financial gain — not when they are made through a machine-learning model and not copies or ‘alterations’ of an existing image. The general reasoning for investigative agencies has, in practice, applied Sections 66C and 66E to deepfake cases is that the created imagery misappropriates the victim's identifying features regardless of whether it was a real image in the first place or an image constructed from fake identifying features. In practice, the general reasoning for investigative agencies has been that the created imagery misappropriates the victim's identifying features, whether the underlying image was real or one created from fake identifying features.²

B. The Bharatiya Nyaya Sanhita, 2023

Although not explicitly targeted at generative AI, the BNS includes a number of broad clauses applicable to deepfakes.

Forgery- Section 336 of the BNS brings together the provisions relating to forgery in the Indian Penal Code and specifically extends to "false electronic records," a change which is significant for synthetic media. A person who fabricates an electronic record — which would include a deepfake video or audio clip — with intent to cause harm or injury to another, or to support a false claim, or to commit fraud, commits forgery and is punishable with imprisonment of up to two years; where the forged record is intended for use in cheating, the punishment rises to imprisonment of up to seven years together with a fine. Under the forgery provisions of the predecessor Indian Penal Code (IPC) Sections 465 and 469, the Delhi Police had registered its first information report in the Rashmika Mandanna matter, and the same BNS provision, Section 336(4) is now believed to be the key criminal law provision for the forgery cases in future. Corresponding BNS provision, Section 336(4), is now understood to be the

²Id.

primary criminal law tool for such cases going forward.³

Cheating by Personation- Section 318 of the BNS outlaws the use of a deepfake voice or video to defraud the victim, and it is clearly the section that should be invoked where a voice or a video is used to convince the victim to give over money or property – for example, when the voice is cloned to defraud a corporate finance department or elderly relatives.

Defamation-Section 356 of the BNS extends the offence of defamation to imputations made by words, signs or visible representations, and will apply where the deepfake makes false assertions or actions concerning a person that adversely affect their reputation.⁴

Criminal Intimidation- Section 351 targets criminal intimidation, which has been defined to include a threat made "by any means" and is sufficiently broad to include a threat to release, or the actual release of, fabricated intimate imagery for extortion or coercion, often referred to as "sextortion."⁵

Public Mischief and Disinformation-Section 353 punishes up to three years' imprisonment, a fine or both for the making or circulation of false statements, rumours or reports likely to cause public fear, alarm or enmity between groups. Combated through this provision is the closest that Indian law has to a disinformation offence, and it has been used in connection with politically motivated deepfakes aimed at fomenting unrest.⁶

Sexual Offences and Voyeurism. Together with the obscenity provisions under Sections 294 and 296 of the BNS, which punish the sale, distribution or electronic dissemination of obscene material, the BNS Section 77 can be extended and applied to situations where a fabricated private image is created and disseminated as if it were real. Organised networks involved in the systematic production or circulation of non-consensual deepfake pornography may also be

³Deepfake Akin to Forgery Under New IT Rules Notification in Week, TRIBUNE INDIA, <https://www.tribuneindia.com/news/india/deepfake-akin-to-forgery-under-new-it-rules-notification-in-week-581864>.

⁴Artificial Intelligence and Criminal Liability in India: Addressing the Legal Vacuum in the Era of Deepfakes and Synthetically Generated Information, RECORD OF LAW (June 6, 2026), <https://recordoflaw.in/artificial-intelligence-and-criminal-liability-in-india-addressing-the-legal-vacuum-in-the-era-of-deepfakes-and-synthetically-generated-information/>.

⁵The Bharatiya Nyaya Sanhita, 2023: Analyzing the Successor to the Indian Penal Code, 1860 (1/3), LEXOLOGY (Jan. 2, 2024), <https://www.lexology.com/library/detail.aspx?g=a9c3dc54-7c09-4421-ba9c-490d31e5bde0>.

⁶AI and Deepfakes: Navigating the Digital Revolution and Its Dark Side, SS RANA & CO. (Mar. 25, 2026), <https://ssrana.in/articles/ai-and-deepfakes-navigating-the-digital-revolution-and-its-dark-side/>.

subject to Section 111 of the BNS, which criminalises organised crime, including cyber-enabled organised crime.⁷

C. The rules in Information Technology as well as the Amendment Rules 2026

In the context of these substantive offences, the Union Government has also exercised its power under the IT Act to impose graduated responsibilities on online intermediaries. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, amended in 2022 and 2023, mandated that intermediaries do their “best endeavours” to prevent the hosting of illegal content, while also issuing advisories in December 2023 and March 2023 to help platforms tackle “synthetic media” and deepfakes.⁸ A more far-reaching amendment followed in February 2026. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 added a new concept of ‘synthetically generated information’ and also imposed labelling obligations on significant social media intermediaries to include the watermark on at least 10 per cent of the surface area of an image or video; or an audible notice on at least 10 per cent of its duration in an audio clip. The 2026 Rules have already shortened the timeline for takedown of harmful SGC, and non-compliant intermediaries can be held liable for such content if they have failed to comply with the specific regulatory requirements, which can include the removal of it. The 2026 Rules have already reduced the time limit for takedown of harmful SGC, with non-compliant intermediaries risking losing the safe-harbour protection normally afforded under Section 79 of the IT Act, to which they may be held liable as if they were the originators of the illegal content. The updated framework specifically requires the removal of “artificially morphed” or highly “invasive” sexual deepfakes within a short timeframe, measured in hours instead of days, due to their particularly severe and time-sensitive impact. Importantly, the 2026 Rules also brought an issue that had long been controversial in this regard, and that had been a disincentive for platforms to proactively police synthetic content: the risk that doing so could be seen as exercising editorial control enough to lose intermediary safe harbour. A new Rule 2(1B) expressly makes it clear that the removal of the unlawful content, including synthetically generated information, by the intermediary in compliance with the Rules shall not be held against the intermediary for Section 79(2) of the IT Act. The purpose of this “Good Samaritan” exception is to align the platforms’ commercial interests more closely with the public interest in removing potentially

⁷Id.

⁸Press Information Bureau, *supra* note 2.

harmful deepfakes in a timely fashion. This "Good Samaritan" exception aims to harmonise better the commercial interests of platforms with the public interest of timely removal of harmful deepfakes.

D. The Digital Personal Data Protection Act, 2023

Because the creation of a deepfake typically involves the processing of a real person's biometric or facial data without consent, the Digital Personal Data Protection Act, 2023 supplies an additional civil-regulatory layer of accountability.

Data fiduciaries — including entities that develop or deploy generative artificial intelligence tools -are obliged to process personal data lawfully and with consent, and the unauthorised use of a person's likeness to train or prompt a deepfake-generating model may constitute a breach attracting substantial monetary penalties.⁹

E. The Bharatiya Sakshya Adhiniyam, 2023 and Evidentiary Complications

The rise of synthetic media also unsettles the law of evidence. The Bharatiya Sakshya Adhiniyam, 2023, which replaced the Indian Evidence Act, 1872, governs the admissibility of electronic records, but neither it nor the jurisprudence built around its predecessor squarely addresses the authentication of media alleged to be, or alleged to have been falsely branded as, an artificial-intelligence fabrication. Two distinct evidentiary risks arise. First, a genuinely fabricated deepfake may be tendered as authentic evidence, whether in a criminal trial or in the court of public opinion, absent robust forensic capacity to detect it. Second, and increasingly documented internationally, a litigant confronted with authentic but damaging audio or video evidence may seek to discredit it by alleging, without proof, that it is an artificial-intelligence fabrication — the "liar's dividend" referred to in Part II.E above. Neither the BNS nor the Bharatiya Sakshya Adhiniyam presently contains a bespoke mechanism for judicial determination of synthetic-media authenticity, leaving courts dependent on ad hoc forensic expert testimony.

⁹Sansalegal, Deepfake Laws in India 2026: Legal Remedies for Victims Under the New IT Rules (Mar. 13, 2026), <https://www.sansalegal.com/post/deepfake-laws-in-india-2026-legal-remedies-for-victims-under-the-new-it-rules>.

IV. THE JUDICIAL RESPONSE: PERSONALITY RIGHTS AND CRIMINAL ENFORCEMENT

Indian courts, most notably the Delhi High Court, have built an evolving civil law doctrine that allows for the protection of civil rights over the unauthorised use of deepfakes: the right of an individual to control the use of their name, voice, image and other distinguishing characteristics of their personality in commercial and non-commercial contexts. Delhi HC in **Anil Kapoor v. Simply Life India**¹⁰ granted an interim injunction to the actor, prohibiting certain entities from using his name, voice, image or his catchphrase through any technology, including AI and deepfakes, for any unauthorised commercial or personal purposes and also directed the Department of Telecommunications and the Ministry of Electronics and Information Technology to issue blocking orders for infringing content. This was done to the actor Amitabh Bachchan in **Amitabh Bachchan v. Rajat Negi**¹¹ in which he had sought a ban on commercial use of his voice and image without his consent. Then came a series of petitions by celebrities like Aishwarya Rai Bachchan, Abhishek Bachchan and filmmaker Karan Johar, and the Delhi High Court said that a celebrity's identity was being exploited without permission, which was not just affecting commercial interest, but also the dignity of living. Although doctrinally not a body of criminal law, this collection of cases does have two practical implications as far as criminal enforcement is concerned. First, the injunctions usually require blocking infringing content and, in a few cases, disclosure of the identity of anonymous uploaders, which can provide the necessary evidence for a later criminal complaint. Secondly, the courts have been regularly finding that the unauthorised use of AI-generated likenesses is a form of identity theft, which provides further guidance for interpreting the applicability of Section 66C of the IT Act and Section 336 of the BNS in criminal proceedings involving the same crime. Turning to the criminal side proper, the Rashmika Mandanna case is the most referenced one wherein the Delhi Police had invoked the forgery and identity theft provisions mentioned in Part III. Prosecutions brought to trial and conviction have rarely been reported, however, partly because of the relative newness of the legislative changes that facilitated them for some time, but also because anonymous or extraterritorial perpetrators are hard to identify in practice.

¹⁰ *Anil Kapoor v. Simply Life India & Ors.*, CS(COMM) 652/2023, slip op. (Del. High Ct. Sept. 20, 2023).

¹¹ *Amitabh Bachchan v. Rajat Nagi & Ors.*, CS(COMM) 819/2022 (Del. High Ct. Nov. 25, 2022).

V. GAPS AND CHALLENGES IN THE EXISTING FRAMEWORK

A. Absence of a Standalone Offence

The most common objection to the Indian framework is structural: there was no BNS provision drafted with the idea of generative AI in mind, and each of the offences mentioned in Part III was conceived to deal with a specific and narrower mischief, namely the alteration of a physical document, the impersonation by another human being, and the circulation of a genuine but non-consensual photograph. Prosecutors are therefore left with the task of shoehorning porn into an overly precise definition, resulting in uneven enforcement based on the provision that is selected and the way that one specific court interprets that provision. A standalone definition of the term 'malicious synthetic media' and a gauge of punishment according to the harm of the synthetic media would provide doctrinal clarity and consistent practice of prosecuting such entities.¹²

B. Mens Rea and the Problem of Intent

Many of the provisions of the BNS and IT Acts that are relevant to deepfakes require proof of a mental state, such as intent to defraud or cause harm, or that the content was false, which can be easily demonstrated in many cases involving extortion and fraud, but is much more difficult in cases involving the creation of content for purposes of satire, parody, or artistic expression, only later to be misappropriated by others for malicious use. A criminal framework that draws too fine a line between the original author and a knowing re-distributor of the work, on one hand, and the unwitting "forwarder" of viral work on the other hand, may create either over-inclusive or under-inclusive consequences for the criminal liability of those who share the content.

C. Anonymity of Perpetrators and Attribution

Deepfake content is often produced and initially shared in anonymous or pseudonymous accounts, which reside on platforms or servers located outside India, and the very tools used to produce the deepfakes can be used without the kind of metadata that can help with traditional cybercrime investigations. Where an intermediary does indeed comply with a takedown notice, it is often not clear who is responsible for the creation of the content that is being taken down

¹²Deep Fakes and Indian Criminal Law, *supra* note 6.

(a predicate for a prosecution for forgery, cheating, and defamation). Mutual legal assistance procedures for the collection of evidence from foreign platforms are slow compared to the speed with which online content goes viral, so by the time an investigation is underway and a potential suspect identified, the damage to the victim's reputation and/or the victim's psychological state could be irreparable. The difficulties in enforcement, including jurisdictional and cross-border challenges. Content can be uploaded to or downloaded from servers located in multiple jurisdictions and generative AI tools are often developed, hosted and operated by foreign entities. Section 75 of the Act provides that the Act also applies to offences committed outside India involving a computer resource that is connected to or accessible from India; however, in practice, this requires the cooperation of foreign law-enforcement authorities and platforms, which is not guaranteed or quick. The 2026 IT Rules amendment does not totally overcome the jurisdictional hurdle of prosecuting individual creators overseas, but solves a part of the accountability problem within India's territory

D. The difficulties in enforcement, including jurisdictional and cross-border challenges.

Content can be uploaded to or downloaded from servers located in multiple jurisdictions, and generative AI tools are often developed, hosted and operated by foreign entities. Section 75 of the Act provides that the Act also applies to offences committed outside India involving a computer resource that is connected to or accessible from India; however, in practice, this requires the cooperation of foreign law-enforcement authorities and platforms, which is not guaranteed or quick. The 2026 IT Rules amendment does not totally overcome the jurisdictional hurdle of prosecuting individual creators overseas but solves a part of the accountability problem within India's territory.

E. The lack of a dedicated legislative instrument for protection against deep fakes.

To establish a specific criminal offence for the malicious generation and dissemination of deepfakes, a private member's bill, the Deepfake Prevention and Criminalisation Bill, 2023, was introduced in Parliament. At the time of writing, the Bill has not been enacted, and the Union Government has opted for a step-by-step approach of making amendments to the IT Rules and awaiting the general provisions in the BNS.

The bigger Digital India Act, which is intended to supersede the IT Act, 2000, is also at a consultative stage and could provide a more comprehensive framework for regulating synthetic

media in the future, commentators added.¹³

F. Chilling Effects and the Risk of Over-Regulation

The threat of over-inclusiveness is a factor that must be taken into account in any reform proposal. Satire, political commentary, film production, historical reconstruction, making things accessible for persons with disabilities and academic research are valid applications of generative artificial intelligence. A criminal provision formulated in an unnecessarily wide manner — such as one that criminalises the creation of a synthetically produced likeness without a narrowly drafted requirement of malicious use or some actual damage — may run afoul of Article 19(1)(a) of the Constitution and be subject to a vagueness challenge like in *Shreya Singhal v. Union of India*,¹⁴ which saw the Supreme Court strike down Section 66A of the IT Act in its wide form.

VI. A CALIBRATED REFORM AGENDA TOWARDS THE FUTURE

Based on the identified gaps above, this article makes five recommendations for reform of the Indian criminal law framework on deepfakes.

* Firstly, Parliament should consider a separate provision in the BNS (a freestanding provision, not the legislation as a whole) that defines "malicious synthetically generated information" and prescribes graduated punishment depending on the nature of the harm caused: sexual exploitation, financial fraud, defamation and electoral disinformation are all different kinds of harm and should be accordingly treated differently.

*Second, any new offence should be accompanied by a clear scienter requirement (knowledge or intent to deceive, plus some reasonable and demonstrable risk of harm) and an explicit statutory defence for parody/satire/artistic work/bona fide research and journalistic use, to ensure that it passes constitutional muster and is not unduly restrictive of legitimate expression.

*Third, the labelling and watermarking requirements under the 2026 IT Rules should be expanded, as far as technically possible, and the requirement for labelling to be added by the intermediary downstream can be circumvented before uploading to the internet.

¹³Jurigram, *supra* note 8.

¹⁴ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

* Fourth, investigative agencies need to have the technical tools and training for detecting deepfakes, and the cybercrime cells need to be specialised for deepfake investigation, including the ability to provide prompt assistance to foreign platforms in time-sensitive cases of non-consensual intimate imagery for which there are no mutual legal assistance protocols.

* Fifth, the Bharatiya Sakshya Adhiniyam, 2023 or any rules made thereunder should be revised to provide a clear evidentiary procedure for authentication or rebuttal of electronically stored records that are suspected of being AI-generated, to protect both against offering fabricated evidence and also against the opportunistic withholding of true evidence as an AI-generated image.

VII. CONCLUSION

So far, India's attempts to deal with the criminal use of deepfake technology have been reactive and incremental: a provision in the forgery law that was reworded to incorporate electronic records, an advisory issued after a scandal went viral, an amendment to the intermediary law to compress the takedown time limits, and a body of civil case law that has been piecemeal and ad hoc, built on the courts' own invention of the definition of forgery. To date, the Indian response to the criminal use of deepfakes has been reactive and incremental: a rewording of the forgery provision to include electronic records, an advisory released after a viral scandal, an amendment to the intermediary law to speed up takedowns, and a series of case law decisions that have been civil, ad hoc and improvised without statutory guidance by the Delhi High Court, which has invented the definition of forgery. Some accountability has been achieved in this patchwork, as illustrated by the cases of the Rashmika Mandanna prosecution and personality rights injunctions granted to Anil Kapoor, Amitabh Bachchan and Aishwarya Rai Bachchan, where the existing law is not vacuous. However, structural tensions between offences framed around physical forgery and human impersonation versus algorithmic and synthetic media created and spread at algorithmic scale have yet to be addressed. With the advent of increasingly more powerful, more affordable, and harder-to-detect generative artificial intelligence tools, the need for a calibrated, harm-specific criminal provision – one that fills the gaps identified in this article without encroaching on legitimate expression – grows ever more pressing. The IT Rules 2026 seem to show that the Indian regulators are prepared to respond to the pace of technological evolution; the challenge before regulators is converting this regulatory responsiveness into a law that is equal to the harms that it must address.

REFERENCES

Amitabh Bachchan v. Rajat Nagi & Ors., CS(COMM) 819/2022 (Del. High Ct. Nov. 25, 2022).

Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023, slip op. (Del. High Ct. Sept. 20, 2023).

Artificial Intelligence and Criminal Liability in India: Addressing the Legal Vacuum in the Era of Deepfakes and Synthetically Generated Information, Record of Law (June 6, 2026), <https://recordoflaw.in/artificial-intelligence-and-criminal-liability-in-india-addressing-the-legal-vacuum-in-the-era-of-deepfakes-and-synthetically-generated-information>.

AI and Deepfakes: Navigating the Digital Revolution and Its Dark Side, SS Rana & Co. (Mar. 25, 2026), <https://ssrana.in/articles/ai-and-deepfakes-navigating-the-digital-revolution-and-its-dark-side/>.

Deepfake Akin to Forgery Under New IT Rules Notification in Week, Tribune India, <https://www.tribuneindia.com/news/india/deepfake-akin-to-forgery-under-new-it-rules-notification-in-week-581864>.

Deepfake Laws in India 2026: Legal Remedies for Victims Under the New IT Rules, Sansa Legal (Mar. 13, 2026), <https://www.sansalegal.com/post/deepfake-laws-in-india-2026-legal-remedies-for-victims-under-the-new-it-rules>.

Deepfake AI Laws in India: Punishment and Precedent, Jurigram (2026), <https://jurigram.com/blog/cyber-law/deepfake-ai-laws-india-punishment>.

Shreya Singhal v. Union of India, (2015) 5 SCC 1.

The Bharatiya Nyaya Sanhita, 2023: Analyzing the Successor to the Indian Penal Code, 1860 (1/3), Lexology (Jan. 2, 2024), <https://www.lexology.com/library/detail.aspx?g=a9c3dc54-7c09-4421-ba9c-490d31e5bde0>.