



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

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

REGULATING DEEPFAKES AND SYNTHETIC MEDIA UNDER INDIA'S NEW CRIMINAL LAWS (BNS)

~*Abhaya*

INTRODUCTION

In November 2023, a video went viral across Indian social media. It appeared to show Bollywood actress Rashmika Mandanna walking into an elevator. Except it wasn't her. It was a digitally manipulated video her face superimposed onto the body of British Indian influencer Zara Patel using artificial intelligence. The video spread across platforms within hours, triggering national outrage, a government advisory, a Delhi Police FIR, and eventually the arrest of a 23-year-old engineer from Andhra Pradesh. Welcome to the world of deepfakes and India's messy, scrambling attempt to regulate them.

The question this article asks is simple but urgent: now that India has replaced the Indian Penal Code with the Bharatiya Nyaya Sanhita, 2023 (BNS), which came into force on 1 July 2024, are we any better equipped to handle deepfakes and synthetic media than we were before?

WHAT ARE DEEPFAKES AND WHY DO THEY MATTER?

Deepfakes are AI-generated or AI-manipulated audio-visual content videos, images, or voice recordings that make a person appear to say or do something they never actually said or did. They are created using machine learning techniques, particularly Generative Adversarial Networks (GANs), which can convincingly swap faces, clone voices, or fabricate entire interactions.

Not all synthetic media are harmful. Deepfakes have legitimate uses in cinema, education, accessibility tools, and digital art. The problem arises when they are weaponized to harass individuals, spread political misinformation, fabricate criminal evidence, create non-consensual pornographic content, or manipulate public opinion during elections. In India, where internet penetration crossed 900 million users and where political deepfakes have already appeared in state elections, the stakes could not be higher.

According to a report by cybersecurity firm Home Security Heroes, deepfake pornography accounts for 98% of all deepfake videos online, with women being the overwhelming victims.

India ranks among the top countries in terms of deepfake-related cybercrime reports filed on the National Cyber Crime Reporting Portal.

THE LEGAL FRAMEWORK BEFORE BNS: IT ACT AND ITS LIMITS

Before examining the BNS, it is important to understand what the existing legal framework looked like and why it fell short.

India's primary legislation for cyber offences is the Information Technology Act, 2000 (IT Act). Several provisions are relevant to deepfakes. Section 66C penalizes identity theft through electronic means, carrying up to three years imprisonment and a fine of up to ₹1 lakh. Section 66D punishes cheating by impersonation using a computer resource, with the same penalty. Section 66E targets the violation of privacy by capturing or publishing private images without consent, with up to three years imprisonment and a ₹2 lakh fine. Sections 67, 67A, and 67B deal with obscene and sexually explicit content in electronic form.

In the Rashmika Mandanna case, Delhi Police invoked Sections 66C and 66E of the IT Act along with forgery provisions. These sections helped register the FIR and eventually lead to an arrest, but they were never designed with AI-generated content in mind. They are technology-neutral provisions stretched to fit a technology-specific problem. The result is a patchwork response rather than a coherent regulatory framework. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 also require platforms to remove illegal content once notified. However, there is no proactive duty to detect deepfakes before harm occurs, no mandatory labelling of AI-generated content, and no clear timeline enforcement mechanism. Advisories issued by the Ministry of Electronics and Information Technology (MeitY) in November 2023 and March 2024 directed platforms to identify and remove deepfakes, but advisories are not law.

WHAT DOES THE BNS SAY ABOUT DEEPPAKES?

The BNS replaced the Indian Penal Code on 1 July 2024. It is India's new criminal code, and its provisions are now the primary lens through which criminal liability for deepfakes must be assessed.

Here is the important thing to understand upfront: the BNS does not mention deepfakes, artificial intelligence, or synthetic media anywhere. Like the IT Act, it is technology neutral. But several of its provisions can be applied to deep-fake-related offences depending on the facts of the case.

Section 319 — Cheating Impersonation: This provision is directly relevant where a deepfake is used to impersonate a real person such as in voice-cloning scams or fake identity fraud. If someone creates a deepfake of a business executive to authorize a fraudulent transaction, Section 319 would apply.

Section 336 — Forgery of Electronic Records: A deep-fake video is, in essence, a false electronic record. Section 336 penalises the creation of forged documents or electronic records with intent to cause harm. This mirrors the old IPC Sections 465 and 469 that were invoked in the Mandanna case.

Section 351 — Criminal Intimidation using Electronic Means: Where a deepfake is created to threaten, coerce, or intimidate a victim — a common tactic in targeted harassment — Section 351 becomes applicable.

Section 353 — Spreading False Information Causing Public Mischief: This is perhaps the most broadly applicable BNS provision to deepfakes. It penalises the spread of false statements, rumours, or reports that cause public mischief or fear. Political deepfakes designed to manipulate elections or incite communal unrest would fall squarely within this section. Additionally, Section 111, which deals with organised crime, can be invoked where deepfake creation is part of a larger cybercrime network.

Section 354 — Sexual Harassment: For non-consensual intimate deepfakes — the most prevalent and devastating form — Section 354 on sexual harassment provides some recourse, though it was drafted in the context of physical harassment and its application to digital synthetic media remains judicially untested.

THE GAPS: WHY BNS ALONE IS NOT ENOUGH

Despite these provisions, the BNS framework for deepfakes has serious limitations that cannot be ignored.

First, there is **no specific deepfake offence**. Every BNS provision applicable to deepfakes requires the prosecution to prove traditional elements — intent to harm reputation, cause public mischief, or intimidate. But deepfakes can cause enormous harm even without a clearly malicious intent — for example, a satirical deepfake that is mistaken for real footage. The law does not adequately capture these scenarios.

Second, the **penalties are mismatched with the harm**. Section 66E of the IT Act carries a maximum of three years imprisonment for privacy violations. For a victim whose career, mental health, and personal life are devastated by a non-consensual deepfake, this is woefully inadequate — especially compared to the Digital Personal Data Protection Act, 2023, which carries penalties of up to ₹250 crore for data processing violations including those involving deepfakes made without consent. Third, there is **no proactive obligation on platforms**. BNS creates criminal liability for individual offenders but places no positive duty on social media platforms to proactively detect or remove deepfakes. By the time a complaint is filed, investigated, and a takedown order obtained, a deepfake can have been viewed millions of times and caused irreversible reputational damage.

Fourth, **attribution and enforcement are extremely difficult**. Deepfakes can be created anonymously using freely available AI tools and uploaded through VPNs. Tracking the creator

— as happened in the Mandanna case only because the creator had linked his fan account to traceable details — is the exception, not the rule.

WHAT INDIA NEEDS: THE WAY FORWARD

India is not starting from scratch. The proposed amendments to the IT Rules in 2026 have begun to address some of these gaps by mandating labelling of AI-generated content, introducing a 3-hour takedown window for deepfake content, and requiring platforms to disclose the identity of deepfake creators to law enforcement. These are meaningful steps.

But they are not enough without legislative backing. What India urgently needs is a standalone deepfake regulation or a dedicated chapter within the IT Act that defines synthetic media clearly, creates specific offences for malicious deepfake creation and distribution, mandates proactive platform detection, and provides proportionate penalties that reflect the severity of the harm caused. Several countries offer instructive models. China introduced specific deepfake regulations in 2022 requiring labelling of AI-generated content. The European Union's AI Act classifies deepfakes as a transparency risk requiring mandatory disclosure. The United States has seen individual states pass deepfake laws targeting electoral and non-consensual intimate content specifically.

India has the legislative momentum, the institutional infrastructure through I4C and CERT-In, and the judicial willingness to address emerging technology harms. What it lacks is the specificity and speed that this threat demands.

CONCLUSION

The BNS represents a significant modernisation of India's criminal law landscape. Its technology-neutral approach means that deepfakes are not entirely outside its reach — Sections 319, 336, 351, 353, and 354 collectively provide a fragmented but real basis for prosecution. But fragmented is the key word. A patchwork of provisions stretched to fit AI-generated harm is not the same as a coherent regulatory response to one of the most dangerous technologies of our time. India cannot afford to wait for the next Rashmika Mandanna moment to act. The law must catch up — specifically, deliberately, and now.

STATUTES

1. Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 319, 336, 351, 353, 354 (India).
2. Information Technology Act, No. 21 of 2000, §§ 66C, 66D, 66E, 67, 67A (India).
3. Digital Personal Data Protection Act, No. 22 of 2023, § 33 (India).
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).

CASE

5. FIR No. registered at PS Special Cell, Delhi Police, against unknown persons u/s 465, 469 IPC & 66C, 66E IT Act (Nov. 10, 2023) (India) [Rashmika Mandanna Deepfake Case].

GOVERNMENT SOURCES

6. Ministry of Electronics & Info. Tech., Advisory to Social Media Intermediaries on Deepfakes (Nov. 7, 2023) (India).
7. Ministry of Electronics & Info. Tech., Advisory to Social Media Intermediaries on Deepfakes (Mar. 2024) (India).