www.ijarp.com ISSN 2456-9992 Page: 01-13

International Journal Advanced Research Publications

Review Article

Volume: 02
Issue: 04

NON-CONSENSUAL INTIMATE DEEPFAKES AND VICTIM REDRESSAL IN INDIA: ASSESSING CRIMINAL LAW REMEDIES UNDER THE BHARATIYA NYAYA SANHITA AND IT ACT POST-2025 AMENDMENTS

*[1]Adarsh Prakash Srivastava [2]Dr. Jyoti Yadav

[1]LLM. (Cyber Law & Cyber 1Security, Amity Law School Lucknow, Amity University Uttar Pradesh Lucknow Campus.

[2]Associate Professor of Law, Amity Law School Lucknow, Amity University Uttar Pradesh Lucknow Campus.

Article Received: 07 March 2026, Article Revised: 27 March 2026, Published on: 17 April 2026

***Corresponding Author: Adarsh Prakash Srivastava**

LLM. (Cyber Law & Cyber 1Security, Amity Law School Lucknow, Amity University Uttar Pradesh Lucknow Campus.

DOI: https://doi-doi.org/101555/ijarp.4878

ABSTRACT

The proliferation of artificial intelligence has made the fabrication of hyper-realistic synthetic media both technically accessible and legally elusive. Non-consensual intimate deepfakes algorithmically generated audiovisual content that superimposes the likeness of a real person onto explicit or intimate material without consent occupy a particularly grievous corner of this problem. In India, the absence of a dedicated deepfake statute has historically compelled prosecutors and victims to navigate a patchwork of criminal provisions drawn from the Bharatiya Nyaya Sanhita, 2023 ('BNS') and the Information Technology Act, 2000 ('IT Act'), supplemented most recently by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 ('2026 IT Amendment'). This paper critically examines the adequacy of these remedies, identifies the structural gaps that persist in the post-2025 legal landscape, and advances a doctrinal argument for bespoke legislative intervention. It argues that while the 2026 IT Amendment represents a normative and procedural advance, the absence of an express criminal offence of non-consensual intimate synthetic imagery continues to expose victims disproportionately women to inadequate redressal, investigative inertia, and re-victimisation.

I. INTRODUCTION: The Crisis of Synthetic Intimacy

When a morphed video of actor Rashmika Mandanna surfaced on social media platforms in November 2023, the public discourse shifted sharply toward the legal vacuum surrounding deepfake technology in India.[1] The video, which superimposed Mandanna's face onto the body of a British-Indian social media creator, Zara Patel, became a flashpoint for national outrage. Delhi Police ultimately filed a First Information Report under Sections 465 and 469 of the Indian Penal Code and Sections 66C and 66E of the IT Act.[2] The arrest that followed driven more by the celebrity status of the victim than by any systematic investigative machinery illustrated both the reactive posture of the State and the doctrinal awkwardness of applying provisions designed for forgery and identity theft to what is, in substance, a sophisticated form of sexual violation.

Non-consensual intimate deepfakes ('NCIDs') represent a distinct and virulent category of technology-facilitated gender-based violence. Unlike traditional non-consensual pornography, NCIDs do not require any prior intimate interaction between perpetrator and victim; a publicly available photograph or video clip is sufficient raw material. The harm is simultaneously reputational, psychological, and existential victims report lasting trauma, occupational disruption, and social ostracism. Despite this, Indian criminal law has until recently approached the phenomenon with conceptual approximations rather than surgical precision.

The present paper proceeds in five parts. Part II maps the existing criminal law architecture applicable to NCIDs under the BNS and IT Act. Part III evaluates the doctrinal fitness of each provision when applied to the specific features of deepfake-based intimate harm. Part IV analyses the 2026 IT Amendment as a procedural and definitional intervention, examining both its contributions and its residual limitations. Part V advances a normative critique and proposes the conceptual architecture for an express NCID offence. Part VI concludes.

[1] Rashmika Mandanna deepfake video row, *BusinessToday* (11 November 2023) https://www.businesstoday.in/technology/news/story/rashmika-mandannas-deepfake-video-delhi-police-register-fir-in-case-after-dcw-seeks-action-405440-2023-11-11 accessed 13 April 2026.

[2] Delhi Police, 'FIR under ss 465, 469 IPC and ss 66C, 66E IT Act registered at PS Special Cell, IFSO Unit' (Delhi Police Statement, 11 November 2023), cited in 'Rashmika Mandanna's Deepfake Creator Arrested', *NewsBytesApp* (20 January 2024) https://www.newsbytesapp.com/news/entertainment/rashmika-mandanna-deepfake-case-delhi-police-nabbed-main-accused/story accessed 13 April 2026.

II. The Existing Criminal Law Landscape

2.1 The Bharatiya Nyaya Sanhita, 2023

The BNS, which replaced the Indian Penal Code with effect from 1 July 2024,[3] does not contain any provision expressly addressing deepfakes, synthetic media, or artificial intelligence-generated content. However, several provisions are capable of application to NCID conduct through interpretive extension.

Section 77 Voyeurism. This provision criminalises the watching, capturing, or dissemination of images of a woman engaged in a private act in circumstances where she would reasonably expect privacy.[4] The section carries a first-offence sentence of not less than one year and up to three years' imprisonment, elevated to a minimum of three years and a maximum of seven years for repeat offenders.[5] Crucially, the BNS clarifies that consent to the initial capture of an image does not constitute consent to its subsequent dissemination making unauthorised sharing a separate and distinct criminal act.[6]

The application of Section 77 to NCIDs, however, is not straightforward. Voyeurism, at its definitional core, involves the observation or capture of a real private act. A deepfake, by contrast, involves the fabrication of a private act that never occurred. The victim was never in the intimate setting depicted; the content is entirely synthetic. A literalist reading of Section 77 would exclude NCIDs because no private act was 'watched' or 'captured' only simulated. Courts would need to adopt a purposive construction to apply this provision to NCID cases, treating the dissemination of a fabricated intimate image as functionally equivalent to the dissemination of an actually captured one. This interpretive gap is not trivial: it invites acquittals and inconsistent judicial outcomes.

Section 79 Assault or Criminal Force to Disrobe. Section 79 criminalises the use of criminal force against a woman with the intention of compelling her to be naked, carrying a sentence of not less than three years and up to seven years.[7] While some scholars have argued that non-consensual digitally manufactured nudity may constitute a constructive form of forced exposure, this provision was designed for physical coercion and stretches conceptually when applied to the purely digital act of synthetically generating a nude image. Any prosecution under this section would face serious definitional challenges.

[3] Bharatiya Nyaya Sanhita 2023 (Act No 45 of 2023), notified by Ministry of Home Affairs, Government of India, operative from 1 July 2024.
[4] Bharatiya Nyaya Sanhita 2023, s 77.
[5] bid.
[6] bid, Explanation 2.
[7] Bharatiya Nyaya Sanhita 2023, s 79.

Section 356 Defamation. Section 356 criminalises imputations made with the intention or knowledge that they will harm the reputation of the person concerned.[8] An NCID clearly satisfies the reputational harm component. However, defamation under the BNS is a non-cognisable and bailable offence, and the bar of proving intentional reputational harm in every case may not capture perpetrators whose motivation is prurience or harassment rather than specifically reputational damage. More critically, defamation provisions are typically invoked for public statements that are false; whether an intimate synthetic image constitutes a 'statement' about the victim remains jurisprudentially unsettled.

Section 351 Criminal Intimidation. Section 351 penalises threatening a person with injury to her person, reputation, or property with intent to cause alarm or compel action.[9] Where NCIDs are used as a tool of coercion demanding silence, money, or sexual compliance under threat of publication Section 351 is directly applicable. This is especially relevant in the growing category of deepfake extortion, where fabricated intimate content is leveraged to blackmail victims. However, this provision addresses only the instrumentalisation of NCIDs for intimidation, not the creation or distribution of such content per se.

Section 111 Organised Crime. Where NCIDs are produced or distributed through coordinated criminal syndicates a pattern increasingly observable in darknet operations Section 111, which criminalises organised crime including cybercrimes committed on behalf of a crime syndicate, becomes applicable.[10] This is a potentially powerful provision for prosecuting large-scale NCID networks, though it requires proof of syndicate membership that individual perpetrators will typically avoid.

Section 316 Cheating. Where deepfakes are deployed to extract property, services, or financial advantage through deception, Section 316 the BNS analogue to IPC Section 420 may apply.[11] This captures the fraud dimension of deepfake misuse but is irrelevant to cases of pure intimate harm.

2.2 The Information Technology Act, 2000

Section 66C Identity Theft. This provision penalises the fraudulent or dishonest use of the electronic signature, password, or any other unique identification feature of another person.[12]

[8] Bharatiya Nyaya Sanhita 2023, s 356.
[9] Bharatiya Nyaya Sanhita 2023, s 351.
[10] Bharatiya Nyaya Sanhita 2023, s 111; Government of India, Press Information Bureau, 'India well-equipped to tackle evolving online harms and cybercrimes' (MeitY, 8 August 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268 accessed 13 April 2026.
[11] Bharatiya Nyaya Sanhita 2023, s 316.
[12] Information Technology Act 2000 (Act No 21 of 2000), s 66C.

In the NCID context, the use of a victim's biometric likeness her face, voice, and bodily features to create a fabricated identity arguably constitutes a form of identity appropriation. The Rashmika Mandanna case was indeed prosecuted in part under Section 66C.[13] However, 'unique identification feature' in Section 66C was designed for digital access credentials and personal identification numbers, not biometric likeness, and extending it to facial superimposition requires jurisprudential creativity.

Section 66D Cheating by Personation. This provision penalises cheating by impersonating any person using any communication device.[14] Where an NCID is used to impersonate the victim for instance, to deceive third parties or to damage her professional relationships Section 66D is applicable. Its limitation is the requirement of a cheating or deceptive purpose, which excludes cases of pure voyeuristic gratification.

Section 66E Privacy Violation. Section 66E criminalises the intentional capture, publication, or transmission of the image of the private area of any person without consent under circumstances violating privacy.[15] This is arguably the most directly applicable IT Act provision to NCIDs, as it focuses on the privacy violation inherent in exposing intimate content. The section carries imprisonment of up to three years or a fine of up to two lakh rupees. However, like Section 77 of the BNS, its drafting contemplates an actual private area of a real person being captured not a synthetically generated depiction of one. The interpretive problem of applying a provision designed for image capture to image fabrication persists.

Sections 67 and 67A Obscenity and Sexually Explicit Material. Section 67 criminalises the publication or transmission of obscene material in electronic form, while Section 67A specifically targets sexually explicit acts and conduct.[16] These provisions carry sentences of up to three years for a first offence and five years for subsequent offences under Section 67, and up to five years for a first offence under Section 67A. Importantly, these provisions do not require non-consent as an element obscenity is regulated as a category of content irrespective of whether the depicted person consented to its creation. This means that NCIDs that are sexually explicit or obscene can be prosecuted under Sections 67 and 67A without confronting the consent-and-fabrication interpretive problem. For this reason, these provisions are arguably the most tactically reliable in NCID prosecutions.

[13] *Rashmika Mandanna Deepfake Row* (n 2).
[14] Information Technology Act 2000, s 66D.
[15] Information Technology Act 2000, s 66E.
[16] Information Technology Act 2000, ss 67, 67A.

III. Doctrinal Fitness: A Critical Assessment

The foregoing mapping reveals a fundamental structural inadequacy: each applicable provision was designed to address a different harm. Taken together, they produce what may be termed 'conceptual coverage without normative precision' the conduct is penalised in some form, but not as the specific wrong it actually constitutes.

3.1 The Fabrication Problem

The central doctrinal lacuna is that Indian criminal law treats intimate harm as requiring either a real private act (Section 77 BNS, Section 66E IT Act) or real identity misappropriation (Section 66C, 66D IT Act). NCIDs involve neither: they fabricate a private act and simulate an identity. This dual-fabrication quality makes NCIDs the paradigmatic harm that slips through the cracks of existing offences. A victim who has never participated in any intimate act is forced to prove harm under provisions designed for those who have.

3.2 Gender Neutrality and Its Discontents

Section 77 of the BNS, as with its predecessor provision Section 354C of the IPC, is explicitly gendered the victim must be a 'woman'. This limitation means that male victims, non-binary individuals, and transgender persons who are subjected to NCID abuse fall outside the protective ambit of this provision altogether. Given that men and gender-diverse persons are increasingly targeted by NCID creators, this gap reflects an outdated legislative assumption that intimate image abuse is exclusively a crime against cisgendered women.

3.3 The Inadequacy of Sentencing

The sentencing regime for the provisions applicable to NCIDs is widely seen as disproportionately mild relative to the severity of the harm. Section 66E of the IT Act carries a maximum of three years' imprisonment or a fine of two lakh rupees a sentence that fails to reflect the enduring and often irreversible psychological harm experienced by NCID victims. A criminal record for the perpetrator, even where obtained, offers the victim no civil remedy or restorative redressal mechanism. The absence of victim compensation provisions in this domain is a conspicuous gap.

3.4 The Evidentiary Challenge

Prosecutions under the existing framework are complicated by evidentiary requirements. Proving non-consent, identifying the creator of an NCID (who may operate behind layers of anonymity, as demonstrated in the Mandanna case where VPN usage delayed

identification),[17] and establishing the chain of custody for digital forensic evidence all present practical barriers. The Bharatiya SakshyaAdhiniyam, 2023 ('BSA'), which replaced the Indian Evidence Act, maintains provisions for electronic evidence and requires maintaining metadata and hash values to prevent tampering during investigation.[18] While this addresses evidentiary procedure, it does not alleviate the investigative challenge of attribution in anonymous online environments.

IV. The 2026 IT Amendment: An Advance, Not a Destination

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026 and operative from 20 February 2026,[19] represent India's first explicit regulatory engagement with synthetic media. The amendment introduces the concept of 'Synthetically Generated Information' ('SGI') under Rule 2(1)(wa), defined as audio, visual, or audiovisual information that is artificially or algorithmically created, generated, modified, or altered using a computer resource, in a manner that such information appears to be real, authentic, or true and depicts or portrays any individual or event in a manner that is, or is likely to be, perceived as indistinguishable from a natural person or real-world event.[20]

4.1 The Three-Hour Takedown Regime

Among the most significant operational reforms of the 2026 Amendment is the establishment of a differential takedown timeline. For non-consensual intimate imagery including morphed and deepfake images intermediaries are required to act within two hours of receiving a complaint or notification.[21] For other unlawful content, the window is three hours. This replaces the previous 36-hour window under the 2021 Rules for intimate imagery, representing an eighteen-fold acceleration of the expected response time. Failure to comply within the prescribed window results in the intermediary losing its safe harbour protection

[17] 'Rashmika Mandanna's Deepfake Video Case: Four Suspects Questioned by Delhi Police', *Outlook India* (18 January 2024) https://www.outlookindia.com/art-entertainment/rashmika-mandanna-s-deepfake-video-case-four-suspects-questioned-by-delhi-police-news-337590 accessed 13 April 2026.
[18] Bharatiya Sakshya Adhiniyam 2023 (Act No 47 of 2023), ss 65A–65B.
[19] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, G.S.R. 120(E), notified 10 February 2026, operative 20 February 2026.
[20] ibid, Rule 2(1)(wa); Khaitan & Co, 'The Regulation of Synthetic Media in India: A Clause-by-Clause Legal Analysis of the IT Rules, 2026 Amendment' (KSK, 19 February 2026) https://ksandk.com/information-technology/it-rules-2026-regulating-synthetic-media/ accessed 13 April 2026.
[21] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, Rule 4(2)(d); India Briefing, 'Global Firms Face Legal Risks Under India's 2026 AI Regulation' (13 March 2026) https://www.india-briefing.com/news/india-ai-regulation-2026-foreign-platform-compliance-42745.html/ accessed 13 April 2026.

under Section 79 of the IT Act, exposing it to direct civil and criminal liability as if it were the originator of the content.[22]

The two-hour window for NCID content represents a significant procedural advance for victim redressal. Rapid takedown is widely recognised as the most effective mitigation for intimate image abuse, as the secondary harms social media sharing, cached content, reputational damage compound dramatically with each additional hour of exposure. From the victim's perspective, this is perhaps the most practically meaningful reform in the 2026 Amendment.

4.2 Mandatory Labelling and Provenance Metadata

The 2026 Amendment requires all SGI to carry prominent visual labels, audio disclosure prefixes, and permanent digital watermarks embedding provenance metadata.[23] Intermediaries providing tools that enable SGI creation are required to deploy automated detection mechanisms and to require user declarations confirming whether uploaded content is synthetic. Platforms must verify these declarations and enforce labelling where content is confirmed as SGI.[24]

For NCID victims, the provenance metadata requirement has a particular investigative value: digital watermarks and metadata trails create a traceable forensic record of the 'computer resource' used to create harmful synthetic content, potentially facilitating perpetrator identification in ways that existing IT Act mechanisms could not support. The 2026 Amendment further requires that where an offence is committed via AI, platforms must disclose the creator's identity to law enforcement,[25] directly targeting the anonymity that has historically shielded NCID perpetrators.

4.3 What the 2026 Amendment Does Not Do

For all its procedural innovations, the 2026 Amendment is an executive instrument a set of Rules made under Section 87(2) of the IT Act. It imposes obligations on intermediaries; it does not create criminal offences. The Amendment does not: (a) define non-consensual intimate synthetic imagery as a standalone criminal act; (b) establish any victim

[22] Information Technology Act 2000, s 79; Mondaq, 'India's 2026 Amendment to IT Rules: Regulation of Deepfakes, AI Content and the Three-Hour Takedown Regime' (25 February 2026) https://www.mondaq.com/india/new-technology/1749116/indias-2026-amendment-to-it-rules-regulation-of-deepfakes-ai-content-and-the-three-hour-takedown-regime accessed 13 April 2026.

[23] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, Rule 4(4)(a)–(c).

[24] Aristo Legal, 'India Cracks Down on Deepfakes: Decoding the February 2026 IT Rules Amendment' (24 February 2026) https://www.aristolegal.co.in/post/india-cracks-down-on-deepfakes-decoding-the-february-2026-it-rules-amendment accessed 13 April 2026.

[25] Insights on India, 'IT Rules Amendment 2026: Deepfake Regulation Explained' (11 February 2026) https://www.insightsonindia.com/2026/02/11/it-rules-amendment-2026/ accessed 13 April 2026.

compensation mechanism; (c) create a right for victims to demand perpetrator identification independent of law enforcement action; or (d) address the jurisdictional complexity that arises when NCID content is created or hosted outside India.

The Amendment is, at its best, a platform governance instrument. Its criminal law interface is indirect intermediaries are warned that non-compliance exposes users to prosecution under the BNS and other laws[26] but this does not constitute substantive criminal reform. The underlying problem of doctrinal fitness examined in Part III remains unresolved.

V. Towards a Dedicated NCID Offence: A Normative Argument

5.1 The Constitutional Foundation

India's constitutional jurisprudence provides a robust foundation for a dedicated NCID offence. In *Justice K S Puttaswamy (Retd.) v. Union of India*,[27] the Supreme Court unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution, encompassing bodily integrity, informational autonomy, and dignity. NCIDs strike at all three dimensions simultaneously: they appropriate the victim's bodily likeness without consent, generate and circulate intimate information about a fabricated version of her, and assault the dignity that the right to privacy is designed to protect.

Article 21, as interpreted by the Court in *Puttaswamy*, imposes positive obligations on the State to establish protective legal frameworks for privacy rights. The persistent gap in criminal law regarding NCID content arguably constitutes a failure to discharge this positive obligation. A dedicated legislative response is therefore not merely desirable as a matter of policy it is constitutionally warranted.

5.2 The Insufficiency of Incremental Interpretation

The Indian judiciary has demonstrated considerable creativity in extending existing provisions to digital harm. The Delhi High Court's orders in *Anil Kapoor v. Simply Life India*[28] and *Amitabh Bachchan v. Rajat Negi*[29] demonstrated the willingness of courts to grant injunctions against AI-generated deepfake misuse on the basis of personality rights and

[26] Mondaq, 'IT Rules 2026 Deepfake Regulation: Three Hour Takedowns and AI Labelling Obligations' (Mondaq, April 2026) https://www.mondaq.com/india/new-technology/1760554/it-rules-2026-deepfake-regulation-three-hour-takedowns-and-ai-labelling-obligations accessed 13 April 2026.

[27] *Justice K S Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

[28] *Anil Kapoor v Simply Life India and Ors* 2023 SCC OnLine Del 6914.

[29] *Amitabh Bachchan v Rajat Negi and Ors*, cited in Lexology, 'Navigating AI Deepfakes: India's Evolving Stance Versus Denmark's Pioneering Bill' (7 August 2025) https://www.lexology.com/library/detail.aspx?g=7a9f914a-2575-4436-b3e6-363d17dad6a2 accessed 13 April 2026.

privacy. In *Ankur Warikoo v. John Doe*,[30] the Delhi High Court addressed AI-generated impersonation for financial fraud through the lens of consumer protection and personality rights. These are significant judicial interventions, but they are civil remedy cases brought by celebrities with access to legal representation. The ordinary victim of NCID abuse the school teacher, the student, the domestic worker has neither the resources nor the standing to bring personality rights litigation before the High Court.

Doctrinal improvisation is not a substitute for legislative certainty. Each incremental extension of an existing provision creates interpretive risk: a differently constituted bench may read the provision differently, a prosecution may fail because the facts do not quite satisfy the stretched interpretation, and perpetrators remain uncertain about the consequences of their conduct. Legislative precision is therefore an imperative of both justice and deterrence.

5.3 Conceptual Architecture of an Express Offence

A dedicated NCID offence should be incorporated into the BNS through amendment and should contain the following essential elements.

Actus reus: The creation, possession with intent to distribute, or distribution of synthetic intimate media defined as any audiovisual, visual, or audio content in which a person's likeness is artificially depicted in an intimate, sexual, or nude context without that person's explicit and informed consent. The offence should encompass the entire production-to-distribution chain: creation, storage, transmission, and the facilitation of access.

Mens rea: The offence should be cognisable at the level of knowledge or reasonable belief that the depicted person has not consented. This standard, rather than a strict intent requirement, prevents perpetrators from claiming ignorance of consent in cases where no consent could reasonably be presumed.

Victim-neutrality: Unlike Section 77 BNS, the offence should be gender-neutral, protecting all persons regardless of sex, gender identity, or gender expression. This aligns with India's evolving anti-discrimination jurisprudence and addresses the documented reality of male and gender-diverse victimisation.

Graduated sentencing: Sentence ranges should reflect both the gravity of the harm and relevant aggravating factors, including: circulation to the victim's professional contacts, distribution to minors, use in extortion, and creation by a person in a position of trust or authority relative to the victim. A baseline custodial range of three to seven years for first

[30] *Ankur Warikoo & Anr v John Doe & Ors* (Delhi High Court, 2024), discussed in Lexology (n 29).

offences, with enhanced penalties for aggravated conduct, would position the offence appropriately within the BNS sentencing architecture.

Victim compensation: The provision should create a statutory right to victim compensation, assessed by the sentencing court on conviction, funded by a dedicated Cyber Harm Victim Compensation Fund administered under the Ministry of Electronics and Information Technology. This is consistent with international best practice in the United Kingdom, where the Online Safety Act 2023 introduced analogous sharing-of-intimate-images offences,[31] and with the trend in domestic violence jurisprudence recognising victim restitution as a component of criminal sentencing.

Extra-territorial jurisdiction: Given the borderless architecture of digital harm, the offence should expressly apply to conduct committed outside India where the victim is an Indian national or resident, consistent with the extra-territorial jurisdiction provisions already present in Section 1 of the BNS.

5.4 Complementary Procedural Reforms

A substantive criminal offence alone is insufficient without structural procedural reform. Three complementary measures are critical:

First, the establishment of dedicated Cyber Sexual Violence Units within State police forces, staffed by trained officers with digital forensics capability and specific sensitivity to the dynamics of intimate image abuse. The experience of the Mandanna case, where the investigating unit was the Intelligence Fusion and Strategic Operations unit of the Delhi Police Special Cell a counter-terrorism and cybercrime unit with no specific victim-support orientation illustrates the mismatch between available institutional resources and the nature of NCID victimisation.

Second, a statutory right of victims to seek an expedited content-removal order from a designated magistrate or cybercrime judicial officer, independent of whether a criminal complaint has been filed. In civil law systems, emergency injunctive relief for intimate image abuse has proven effective, and a similar mechanism under Indian procedural law perhaps through amendment to the Bharatiya Nagarik Suraksha Sanhita, 2023 would provide victims with a self-directed remedy that does not depend on police action.

Third, mandatory training for prosecutors and judicial officers on the technical characteristics of NCID content, including the forensic interpretation of provenance metadata, deepfake

[31] Online Safety Act 2023 (UK), ss 188–191 (offences of sharing or threatening to share intimate photographs or films).

detection tools, and the psychological impact of synthetic intimate image abuse. Technical illiteracy in the courtroom is a systemic barrier to justice in this domain.

VI. CONCLUSION

India's existing criminal law architecture applicable to non-consensual intimate deepfakes is characterised by doctrinal improvisation rather than normative precision. The BNS and IT Act together provide a patchwork of provisions voyeurism, obscenity, identity theft, defamation, privacy violation that approximate coverage of NCID conduct without directly addressing it. The 2026 IT Amendment is a meaningful advance in platform governance and takedown procedure, but it is fundamentally an intermediary regulation instrument, not a criminal law reform. The two-hour takedown window for intimate content, the mandatory SGI labelling regime, and the provenance metadata requirements all strengthen the enforcement ecosystem around NCID harm, but they do not create the express criminal offence that the gravity of the harm demands.

The constitutional imperative derived from *Puttaswamy*, the disproportionate victimisation of women and gender-diverse persons, the psychological severity of deepfake intimate abuse, and the inadequacy of celebrity-litigation as a proxy for systemic legal protection together make an unanswerable case for legislative intervention. An express NCID offence, incorporated into the BNS with gender-neutral drafting, graduated sentencing, victim compensation, and extra-territorial reach, is the minimum that a rights-responsive legal system owes to the growing population of persons whose dignity is daily violated by synthetic intimate content.

The law, as it stands, asks victims of one of the most technologically sophisticated forms of sexual harm to seek redress under provisions designed for film photography, typewritten forgeries, and analogue identity theft. This is not merely inadequate it is a categorical failure of the State's positive obligation to protect the right to privacy and dignity under Article 21. The moment for legislative correction is not approaching. It has already passed.

BIBLIOGRAPHY

Cases

1. *Amitabh Bachchan v. Rajat Negi*
2. *Anil Kapoor v. Simply Life India*
3. *Ankur Warikoo v. John Doe*
4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*

Statutes and Legislation

India

1. Bharatiya Nagarik Suraksha Sanhita, 2023
2. Bharatiya Nyaya Sanhita, 2023 (specifically Sections 1, 77, 79, 111, 316, 351, and 356)
3. Bharatiya SakshyaAdhiniyam, 2023
4. Constitution of India (specifically Article 21)
5. Indian Evidence Act
6. Indian Penal Code, 1860 (specifically Sections 354C, 420, 465, and 469)
7. Information Technology Act, 2000 (specifically Sections 66C, 66D, 66E, 67, 67A, 79, and 87(2))

International

1. Online Safety Act 2023 (United Kingdom)

Rules and Regulations

1. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026
2. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021