

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

CRIMINAL LIABILITY FOR DEEPFAKE TECHNOLOGY **IN INDIA A CRITICAL REVIEW OF THE EXISTING** **LEGAL FRAMEWORK**

AUTHORED BY - RAMESH KUMAR. T

LL.M (Criminal Law) Final Year Student Crescent School of Law

B. S. Abdur Rahman Crescent Inst of Science & Technology, TN

ABSTRACT

The fast-moving development of artificial intelligence has given rise to deepfake technology, hyper-realistic synthetic media that can impersonate persons with terrifying precision. Deepfakes, while having artistic and economic potential, have been weaponized for criminal purposes, including non-consensual pornography, identity theft, financial fraud, defamation and political propaganda. India's large digital population has seen a worrying rise in deepfake-related crimes, revealing major flaws in the current criminal justice system. This doctrinal study critically evaluates the sufficiency of India's current legal framework, primarily the Information Technology Act, 2000, the recently enacted Bharatiya Nyaya Sanhita, 2023 and other rules and regulations to punish deepfake-enabled offenses. The study has three objectives: to develop a conceptual framework for the illegal abuse of deepfakes, to identify legislative lacunae and enforcement bottlenecks and to suggest specific reforms for improved criminal accountability and victim protection. The article adopts a purely doctrinal approach in analysing statutory provisions, judicial pronouncements, advisory guidance and comparable legislative models. The study finds that the laws that exist to address deepfake harms are scattered and analogical, and no statute specifically criminalises the creation and distribution of a deepfake. Technical anonymity, the lack of standardised forensic techniques, jurisdictional ambiguity in cross border crimes and evidentiary complexity that challenge the traditional burden of proof are some of the significant challenges facing law enforcement and courts. The report suggests that India should move beyond a piecemeal application of broad cybercrime rules and adopt a dedicated deepfake-specific offense regime. Key measures will include outlawing non-consensual synthetic intimate imagery, requiring content produced by AI to be labelled, greater accountability for intermediaries, and the creation of specialist digital investigation units. A strong legal response is not only desired but also necessary to protect individual dignity, electoral integrity and public confidence in the digital economy.

Keywords: Deepfakes, Criminal Liability, Information Technology Act, Bharatiya Nyaya Sanhita, Synthetic Media, Cybercrime, Victim Protection

Introduction

Deepfake technology is a paradigm leap in the generation and manipulation of digital information. Deepfakes, enabled by generative adversarial networks (GANs) and advanced machine learning, may superimpose a person's face, voice and mannerisms on to fake audio-visual content to the point that it is very difficult to detect.¹ The technology has democratized swiftly, from a research lab and innocent amusement to freely available mobile apps and open-source software putting the tools for near-perfect impersonation in the hands of every internet user.² The societal fallout is severe: a single malevolent deepfake video can destroy reputations, destabilize financial markets, spark communal conflict, or influence election results.

India, with more than 900 million internet users and a highly digitized public realm, is quite vulnerable.³ It began with non-consensual sexual movies of female celebrities, journalists and regular women, then spread to political disinformation and financial schemes. The country has seen a significant increase in deepfake instances. The widely circulated Deepfake video of actor Rashmika Mandanna in 2023 was a watershed moment with urgent calls for regulatory intervention. Even with public protest, the legal reaction remains tentative and fragmented. The architecture of criminal law, principally the Bharatiya Nyaya Sanhita, 2023 (BNS) (which repealed the Indian Penal Code, 1860 and the Information Technology Act, 2000 (IT Act)) does not make any specific mention of deepfakes. Existing categories such as defamation, obscenity, identity theft, or cheating by personation are employed to punish offenses, none of which were ever intended to deal with the specific harm produced by AI-generated synthetic media.⁴

This doctrinal study attempts to critically evaluate the Indian criminal liability framework in the light of deepfake technology. It is framed around three specific objectives: first, to define

¹ Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", 107 California Law Review 1753, 1758 (2019).

² Mika Westerlund, "The Emergence of Deepfake Technology: A Review", 9 Technology Innovation Management Review 39, 41 (2019).

³ Internet and Mobile Association of India, "Digital India Report 2024" 12 (IAMAI, 2024).

⁴ Arvind Narrain, "Cybercrimes and the Limits of the Information Technology Act", 7 NLUD Journal of Legal Studies 25, 33 (2022).

the concept and typologies of criminal abuse of deepfakes; second, to identify substantive legal gaps and enforcement challenges that impede investigation and prosecution; and third, to propose concrete legislative and institutional reforms to strengthen criminal liability and victim protection.

The research topics that guide the inquiry are:

- (1) What obstacles are law enforcement agencies and courts confronted with when investigating and prosecuting deepfake-related offences?
- (2) Is the present legislative framework, specifically BNS and the IT Act, sufficient to tackle the crimes related to deepfakes?

The paper employs a purely doctrinal methodology, analyzing primary sources, including statutory texts, judicial decisions, parliamentary debates, executive advisory, as well as secondary scholarly discussion and comparative legal resources. The study is important as it tries to fill the gap between the technological reality and the normative legal reaction at a time when India's digital jurisprudence is being altered by the new criminal codes and increasing intermediary rules. The article proceeds to unravel the technological and criminological features of deepfakes, map the existing legal provisions, expose their flaws and suggest a detailed reform strategy.

Deepfake Technology: What You Need to Know about Criminal Misuse

A. What are Deep Fakes?

Deepfakes are synthetic material — photos, audio or video — made using algorithms based on deep learning to plausibly replace the likeness of one person with that of another or to construct wholly fictitious but credible representations.⁵ The word, a mash-up of “deep learning” and “fake,” was coined in 2017 when a Reddit user released AI-generated porn movies.⁶ Technically, most deepfakes use Generative Adversarial Networks, where two neural networks, a generator and a discriminator, fight to create increasingly authentic outputs. The most typical uses are face-swap, lip-synch and voice cloning, which just require publicly available data such as social media photos or voice samples.⁷ The pace at which these

⁵ OECD, “Artificial Intelligence and Synthetic Media: Policy Considerations”, OECD Digital Economy Papers No. 340, 8 (2023).

⁶ Karen Hao, “The Origin Story of Deepfakes”, MIT Technology Review, Oct. 12, 2020, available at: <https://www.technologyreview.com/2020/10/12/1009949/origin-of-deepfakes> (last visited on July 27, 2026).

⁷ Siwei Lyu, “Deep Fake Detection: Current Challenges and Next Steps”, 31 Journal of Visual Communication and Image Representation 102572 (2020).

technologies have been commodified has reduced the entry barrier; now, anyone with a smartphone can create a convincing deepfake in minutes, making detection and attribution extremely tough.⁸

B. Typology of Criminal Abuse

Criminal use of deepfakes can be categorized into four overlapping areas. The first, and most common and gendered type of deepfake crime, is non-consensual synthetic pornography, which overwhelmingly targets women. Victims' faces are overlaid on pornographic material without their knowledge, leading to serious psychological distress, social ostracism and professional harm. Second, deepfake audio or video is used in identity theft and financial fraud to impersonate corporate executives, family members or public officials to facilitate fraudulent fund transfers, phishing attacks and contract forging. A deepfake video call impersonating the CFO of a multinational firm in 2023 resulted in a multi-million dollar loss in Hong Kong, a situation that is easily reproducible in India's developing digital economy. Third, defamation and reputational injury include creating compromising or inflammatory content to defame individuals, political adversaries, or commercial competitors. Fourth, electoral and societal disinformation refers to the use of deepfakes to promote false narratives, inflame community tensions, or influence voting behaviour, and hence threatens democratic integrity and public order. Each of these categories, however, offers different legal issues as the harm is often exacerbated by the viral nature of social media platforms where content is disseminated in an irreversible manner before any legal remedy can be sought.

A Critical Analysis of Criminal Liability Regime in India

The Information Technology Act, 2000

The principal legislation regarding cyber offenses is the IT Act (amended in 2008). There are other clauses that can be enforced against deepfake-related crimes, albeit indirectly. Section 66E criminalizes the purposeful capture, publication or transmission of a "private area" of any person without his or her agreement. But it is limited in that the wording only speaks of photos of "private areas" and does not include the synthetic manufacture of a non-private but compromising visual.⁹ Section 66D makes cheating by personation by using any communication device or computer resource, an offence. This may include deepfake-based financial fraud where impersonation results in unjust gain. Section 66C (Identity theft) This

⁸ Henry Ajder et al., "The State of Deepfakes 2023" 6 (Deep trace Labs, 2023).

⁹ The Information Technology Act, 2000 (Act 21 of 2000), s. 66E.

section deals with the fraudulent or dishonest use of another person's electronic signature, password or any other unique identification feature. The term "unique identification feature" is a broad one, but courts have yet to construe it to include biometric voice patterns or face biometrics acquired and mimicked by AI.¹⁰

Sections 67, 67A and 67B are the three cyber-obscenity and sexual explicit content crimes. Section 67 penalises publishing or transmitting obscene content in electronic form. Section 67A especially targets material featuring a "sexually explicit act" while Section 67B criminalises child pornography. Section 67A could be used to punish non-consensual deepfake pornography if the created film shows a sexually explicit conduct, although the clause does not criminalise the process of making a deepfake, only its publication or transmission. Moreover, lack of consent by the victim is not an element of the offence under these sections; the prosecution must prove that the item is sexually explicit in itself. Paradoxically, a non-sexual but profoundly humiliating deepfake (e.g. representing a person committing a crime) would not be caught by Sections 67–67A, leaving only conventional defamation remedies.

The IT Act also places due-diligence responsibilities on intermediaries under Section 79 read with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Intermediaries are required to take down illicit content upon actual knowledge or court order. However, the reactive nature of this process and the enormous volume of content created by users make the ex-post removal mostly ineffective.¹¹ A deepfake video could be up there for hours or days, doing irreparable harm, before it receives a takedown request. In March 2023, the Ministry of Electronics and Information Technology issued an advisory asking social media platforms to remove deepfakes within 24 hours of a complaint. A subsequent advisory in November 2023 reiterated the requirement to take down AI-generated synthetic content that violates the IT Rules. These advisories indicate the executive's intent, but they are not statutes and do not create new criminal responsibilities.

B. Bharatiya Nyaya Sanhita, 2023

The BNS updates certain parts of criminal law but does not establish a separate crime for deepfakes and takes effect on July 1, 2024. Chapter XVIII deals with offences connected to documents and property markings and has increased rules on deception and forgery which may be of tangential application. Section 318(2) deals with punishment for cheating by personation.

¹⁰ The Information Technology Act, 2000 (Act 21 of 2000), s. 66C; see also *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

¹¹ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3.

This applies to any person who “falsely represents” a person. Section 318 could apply where the attacker utilizes a deepfake video call to impersonate a bank official and compel the victim to transfer monies.¹² But the wording “falsely represents” assumes a live portrayal to a particular victim, rather than a synthetic film being disseminated to the public at large. The IPC’s approach to defamation continues in Section 356 of the BNS, which punishes anybody who makes an imputation intending to injure reputation. A deepfake that damages a person’s reputation could result in a prosecution for defamation, but criminal defamation is a non-cognizable, bailable and compoundable offence, and the duty of inquiry is in the first instance on the private complainant and not on the state machinery. Also, truth is an acceptable defence if it is in public interest, an argument that could be used in political deepfake instances. Sections 294 to 296 deal with obscenity and outraging modesty but they are largely aimed at acts done in public places or by words and gestures. They are not well adapted to electronic transmission of deepfakes. The BNS also adds a new charge of ‘organised crime’ under Section 111, but applying it to deepfake networks would require proving ongoing unlawful behavior and syndicate structure – a level too high for isolated deepfake creators. Most crucially, the BNS does not treat the non-consensual development of a synthetic intimate image as a separate damage, and the creation of a deepfake privately stored on a hard drive is completely outside the reach of criminal consequence unless it is later disseminated.¹³

C. Other Regulatory and Proposed Frameworks

The Digital Personal Data Protection Act, 2023, which goes beyond the IT Act and BNS to provide data protection, sets up a consent-oriented data protection framework, but does not prohibit the exploitation of personal data for deepfake production; its sanctions are mostly administrative and civil.¹⁴ The Digital India Bill, set to replace the IT Act, is currently under negotiation and is expected to include explicit rules for synthetic media and algorithmic accountability, but its timing for enactment is unclear. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 established the notion of fact-checking units, but these are only for content related to the government and do not provide criminal remedies to individual victims.¹⁵

The present legislative framework is therefore a patchwork of general statutes that can deal with some aspects of the deepfake crime but do not prosecute the primary injury, which is the

¹² The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 318(2).

¹³ Aparna Chandra, “Criminal Law and the Digital Body”, 6 Indian Law Review 201, 215 (2022).

¹⁴ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), Preamble and s. 8.

¹⁵ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023.

non-consensual creation of a person's likeness. The law responds to downstream repercussions, not the upstream behavior, resulting in a substantial responsibility void.

Enforcement Challenges and Legal Gaps

A. Gaps in the Substantive Criminal Law

The most obvious difference is the lack of a statutory definition of deepfake and a specific crime for creating deepfake for malevolent reasons.¹⁶ Existing rules compel the prosecution to fit deepfake activity into analogical boxes – obscenity, cheating, defamation – each with its own legal obligations and defences ill-suited to the technology. For instance, non-consensual deepfake pornography does not fall squarely under the “private area” requirement of Section 66E or the “sexually explicit act” requirement of Section 67A when the original image was harmless. Furthermore, the law does not discriminate between consensual synthetic media for satire or artistic expression and weaponized deepfakes. Overbreadth problems arise if current prohibitions are pushed too far.

The BNS is just as tight-lipped on the threat of election-related deepfakes. While the Representation of the People Act 1951 penalises certain forms of election malpractice, there is no express restriction on synthetic audio-visual content designed to mislead voters. The Election Commission's existing rules on political advertising are largely geared towards print and broadcast media, and lack sufficiently strong measures to prevent AI-generated disinformation being spread via encrypted messaging platforms.¹⁷

Another important shortcoming is the lack of victim-centric provisions. The IT Act and BNS do not demand the rapid removal of non-consensual deepfakes from all platforms, nor do they provide for temporary reliefs such as preservation orders or a compensation fund for victims. Too often victims are forced down the long road of civil litigation, which is fiscally and emotionally expensive.

B. Procedural and Investigatory Hurdles

It is difficult to investigate crimes that involve deepfakes. First, anonymity and pseudonymity are intrinsic to the digital ecosystem; criminals commonly utilize Virtual Private Networks (VPNs), onion routing and encrypted messaging services, making IP-based tracing problematic. Indian law enforcement authorities lack sophisticated de-anonymization tools and the forensic competence to locate the originators of deepfakes which use anti-forensic tactics

¹⁶ Joint Parliamentary Committee, “Report on the Personal Data Protection Bill, 2019” para. 12.8 (2021).

¹⁷ Election Commission of India, “Guidelines on Political Advertising” para. 5 (2023).

such as metadata stripping and steganography.¹⁸

Second, cross-border jurisdictional complexity greatly hampers investigations. A deepfake developed on a server in a foreign jurisdiction, published through a platform incorporated in a third country, and targeted towards an Indian victim generates a complex web of applicable laws and mutual legal aid treaties. Section 75 of the IT Act applies to acts committed outside India if the act is conducted using a computer located in India. But enforcement is dependent on bilateral co-operation, which is slow and sometimes ineffectual.¹⁹

Third, local police stations are hampered by resource and capability limitations. Big cities have cyber crime cells but most of the First Information Reports (FIRs) of cyber offences are lodged in normal police stations where officers are not trained in digital forensics. The National Cybercrime Reporting Portal is a positive move however it is solely for complaint registration and not active investigation. The National Cyber Forensic Laboratory's network is in its infancy and poorly equipped to deal with the volume and sophistication of deepfake evidence. Fourth, the platforms' lack of cooperation exacerbates the problem. Intermediaries routinely rely on data privacy regulations of their parent jurisdictions to stall or refuse information requests. The appointed grievance officers under the IT Rules often give templated responses rather than meaningful assistance. The 24-hour takedown advisory is better observed in breach than in observance, particularly outside of work hours.

C. Evidentiary, Forensic Challenges

The evidentiary challenges in setting up a deepfake offense in court are very specific. Digital evidence is documentary evidence under Section 3 of the Indian Evidence Act, 1872 (now replaced by the Bharatiya Sakshya Adhiniyam, 2023) and is admissible subject to the certification requirements of Section 65B. But the authenticity of a digital record becomes highly questionable when the entire premise of the offence is fabrication. The prosecution needs to present specialized forensic evidence to demonstrate that a video is a deepfake, not an actual recording. However, India faces a serious dearth of competent digital forensic examiners. The few available are clustered in private labs and their reports typically do not reach the evidentiary requirements required for criminal conviction.

Also deepfake detection methods are not conclusive but probabilistic, they give confidence scores rather than binary outcomes. This epistemic ambiguity might be used by defence counsel to raise reasonable doubt. The machine produced probabilities do not fit well with the binary

¹⁸ National Crime Records Bureau, "Crime in India 2022: Cyber Crimes Report" 112 (2023).

¹⁹ The Information Technology Act, 2000 (Act 21 of 2000), s. 75.

standard of proof beyond reasonable doubt of the adversarial system. Courts have yet to develop a coherent jurisprudence for the appraisal of AI-generated evidence or the admission of detection-tool outputs.

The burden of proof also creates human rights issues. For example, in obscenity trials the defence would seek to show that the victim had consented to the underlying image in the first place, and engage in intrusive cross-examination.²⁰ The law fails to distinguish between a consensual image later weaponised through deepfake production and a self-published obscene image, leaving victims at risk of re-victimisation in the courtroom.

D. Barriers of an Institutional and Societal Nature

Stigma, fear of being blamed for the crime and lack of confidence in the criminal justice system leads to pervasive under-reporting. Women, most of the victims of deepfake pornography, are generally silent in the face of public scrutiny. Even if FIRs are filed, the trial process is excruciatingly lengthy. In the instance of cybercrime in India, the conviction rate is less than three per cent, which further disincentivises victims from seeking legal remedies.

Finally, regulatory fragmentation between the Ministry of Home Affairs, and the Ministry of Information and Broadcasting, leads to jurisdictional overlaps and buck-passing, delaying timely executive action. Without a coordinated response among multiple stakeholders, enforcement will be reactive, piecemeal and mainly symbolic.

The Judicial Reaction and the Dilemmas of Interpretation

Indian courts have started to address problems associated to deepfakes, mostly via the prism of constitutional privacy rights rather than criminal adjudication. In *K.S. Puttaswamy v. Union of India*,²¹ the Supreme Court recognised right to privacy as a fundamental right which includes informational privacy and right to control one's own image. This offers a solid jurisprudential basis to argue that non-consensual deepfakes breach Article 21, although the declaration does not necessarily entail criminal culpability until legislated by the Parliament.

In a landmark public interest action before the Delhi High Court on the Mandanna deepfake, the court had urged the government to handle the issue with haste and propose special legislation. But the court did not lay out required standards, respecting the separation of powers.

²⁰ Rukmini Sen, "Victimisation in Obscenity Trials: A Feminist Critique", 52 *Journal of Indian Law Institute* 459 (2020).

²¹ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

In the case of morphed pornographic photos, the lower courts have dismissed bail pleas under Section 67A of the IT Act, but these judgments have been based on the “sexually explicit” nature of the content and not the act of synthetic alteration per se. The basic interpretive challenge remains: judges are required to extend legislative language to accommodate technology harms which the legislature never envisioned, at the risk both of over-criminalization and of legal uncertainty.

Considering the norm of legality in Article 20(1) of the Constitution, it is reasonable that the judiciary is reluctant to repair legislative gaps through purposive interpretation. Any attempt to ban deepfake activities by judicial decree would be open to constitutional scrutiny. Hence, legislative involvement is both constitutionally and practically unavoidable.

Suggestions and Enhancements

1. Creation of a Specific Chapter on Deepfake Offences

The Parliament should enact a comprehensive legislative change either through the forthcoming Digital India Bill or as a separate Deepfake (Prohibition and Regulation) Act. The law should define “deepfake” as clearly as “any audio, visual, or audio-visual media created or altered by artificial intelligence techniques to depict a person saying or doing something that did not happen, where such depiction is likely to deceive a reasonable viewer or listener.” The substantive offenses should cover: (a) production of a non-consensual intimate deepfake with intent to harm, punishable with imprisonment up to five years and fine; (b) dissemination of any deepfake known to be false with intent to deceive, harm reputation, or incite violence; (c) use of a deepfake for financial fraud or identity theft; and (d) distribution of election-related deepfakes during the campaign silence period. We need to create separate penalties for repeat offenders and for organized deepfake development rings.

2. Enhancing the obligations of Intermediaries

The Intermediary Guidelines should be upgraded to statutory obligations to block in real time deepfakes flagged by court-appointed digital fact-checking bodies; to mandate integration of AI-content provenance tools (like Coalition for Content Provenance and Authenticity standards); and to require 24-hour takedown orders with financial penalties for non-compliance. Platforms should be forced to label content created by AI clearly and keep logs of requests to alert deepfakes.

3. Forensics and Institutional Capacity Building

The government should create a National Deepfake Forensics Unit under the Ministry of Home Affairs, armed with the latest detecting software and trained digital forensic analysts. Deepfake investigation wing should be dedicated to each state cybercrime cell. The network of Central Forensic Science Laboratories should be strengthened with regional laboratories specializing in audio-visual authentication. A central store of known deepfake fingerprints (hash values) could be kept and shared with intermediaries to enable automatic blocking.

4. Procedural Changes to Help Victims

The amendments to the BNS and the Bharatiya Nagarik Suraksha Sanhita, 2023 should lead to non-consensual deepfake pornography being a cognisable, non-bailable offence, so that the police can take swift action. A victim compensation plan must be set up, supported by penalties imposed on intermediaries and perpetrators, to cover legal costs, therapy and rehabilitation. Deepfake cases should be directed to special fast track courts for cyber-offences against women and vulnerable groups. A legal right to have intimate deepfakes de-indexed from search engines must be recognised, comparable to the “right to be forgotten” upheld by the Supreme Court in *Puttaswamy*.

5. Capacity Building and Awareness Raising

Deepfake detection, collecting of digital evidence and victim-sensitive handling ought to be made mandatory training for judges, prosecutors and police personnel. Public awareness efforts, especially targeting adolescents and young people, should inform them of the legal ramifications of producing and disseminating deepfakes.

6. International Collaboration

Given the transnational nature of deepfake crimes, India needs to advocate for an international convention on synthetic media crimes under the United Nations Office on Drugs and Crime and broaden mutual legal assistance treaties to encompass expedited preservation and disclosure of digital evidence stored in foreign jurisdictions.

7. Responsible AI Regulatory Sandbox

Finally, besides criminalisation, a regulatory sandbox for ethical AI should promote the creation of sophisticated provenance-verification tools while protecting legitimate applications of synthetic media in arts, satire and education, thus balancing regulation and innovation.

Conclusion

Deepfake technology is a double-edged sword. It is a marvel of artificial intelligence, but when exploited it may cause severe and permanent hurt to individual dignity, democratic processes and social harmony. The doctrinal analysis carried in this paper affirms that the existing structure of criminal law in India, as evidenced in the BNS, the IT Act and ancillary rules, is structurally unable to meet the complex nature of deepfake-related offenses. The law punishes the downstream implications of deepfake misuse, such as defamation or obscenity, but does not criminalise the fundamental act of non-consensual synthetic fabrication, leaving a dangerous void at the heart of the digital system.

Technical anonymity, forensic incompetence, fragmented jurisdiction and outmoded evidentiary rules combine to hinder efficient investigation and prosecution, severely limiting the power of enforcement agencies and courts. The adversarial judicial system's requirement for binary certainty clashes with the probabilistic outcomes of detection algorithms, creating a divide between technical reality and legal proof. Victims, mostly women, are twice victimised, first by the deepfake and then by a court system that struggles to provide quick, compassionate and effective remedy.

The way forward requires immediate, coordinated legislative action. India needs to introduce specific criminal offences for development and transmission of malicious deepfakes, enforce requirements on intermediaries, invest extensively in forensic infrastructure and put victim protection at the core of procedural and substantive law. The constitutional promise of dignity and privacy in life so eloquently proclaimed in K.S. Puttaswamy will be a hollow victory until the law adapts to meet the age of synthetic reality. With the digital environment moving at warp speed, legislative stasis is a luxury this nation can no longer afford. The time to act is now, not merely to punish the criminals, but to assert that in a democratic society, truth, consent and human integrity are non-negotiable.