INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

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.

ISSN: 2582-6433

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

ISSN: 2582-6433

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.

ISSN: 2582-6433

AI – GENERATED SEXUAL DEEPFAKES AND GENDER JUSTICE IN INDIA: EXAMINING CONSENT, PRIVACY AND CRIMINAL LIABILITY

AUTHORED BY - KARUNA BHARDWAJ & HIMANSHI HUDDA

Abstract

A woman can now be represented in sexually explicit images created with AI if only one of her images is available. This paper looks into the responses of Indian Law towards deepfakes and non-consensual intimate imagery. It asserts that the current system, which is made up of Bharatiya Nyaya Sanhita (2023), the Information Technology Act (2000), the Digital Personal Data Protection Act (2023), and the intermediary rules in 2026, is underpinned by three faulty presumptions: that the offending image depicts a real incident, that the problem is that of obscenity as opposed to consent's absence, and that harm occurs if people believe the image. In a doctrinal and comparative analysis, the paper uses a rights-based approach based on Puttaswamy on privacy and dignity and outlines the shortcomings of the current law, and what changes need to be made.

KEYWORDS: Deepfakes, Non-Consensual Intimate Imagery, Gender Justice, Sexual Privacy, Consent, Intermediary Liability.

I. Introduction

All it takes is a single snapshot from a social media account to create a highly realistic, sexualised image of the person concerned. The technology involved is easily available and calls for no technical skill. The way this technology is used is strongly gendered in nature. One of the earliest surveys of deepfake videos found that roughly ninety-six per cent of the videos made with deepfakes were pornographic and showed women against their will.[1].

There is no statute that speaks directly about this wrong. The victim needs to grapple with the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology Act, 2000 (IT Act), the Digital Personal Data Protection Act, 2023 (DPDP Act), the revised intermediaries' guidelines

[1] Henry Ajder et al., Deep trace, The State of Deepfakes: Landscape, Threats, and Impact (2019). The data pertains to the sample analysed in 2019 and represents a trend instead of an up-to-date statistic.

ISSN: 2582-6433

of 2026, and the ever-increasing case law from the High Courts. Three questions arise out of this paper. What exactly is the wrong done to the person targeted by a sexual deepfake, and can it be expressed through the principles of consent, privacy, and dignity? Second, how well does the current statutory framework in India address this wrong? And third, which form of reform would be proportional to it?

The thesis argues that Indian law rests on three assumptions that deepfakes undermine: first, that the offending image proves an event occurred; second, that the wrongdoing is obscenity rather than a lack of consent; and third, that the victimized party is someone who takes the image at face value. The paper employs a doctrinal method grounded in statutes, rules, case law, and literature. It uses comparative legislation as well and sets out the state of the law as of October 2026. This field of study is doctrinal, as it will investigate whether criminal law and constitutional law are able to safeguard autonomy in cases where the harm stems not from the disclosure of truth but from the very construction of the concept of the individual's sexuality. It is also practical since it addresses a problem where the victims have to resort to inefficient, unreliable and expensive means of redress. The topic covers sexually explicit deepfake images involving real adults. Child sexual abuse material and deepfakes driven by political or satirical motives raise distinct issues and are addressed only when relevant.

II. Conceptual Framework: Deepfakes and Violence Based on Gender

A. The technology

The word "deepfake" describes fabricated media content that is generated through machine learning. Earlier technologies used generative Adversarial networks in which two neural networks learn to outdo each other until one comes up with an excellent forgery.[2] Today, technologies involve face swap apps, diffusion models used to create images based on prompts and pictures and “modify” apps that generate a fake naked picture from a clothed picture[3]. In all cases, no event is captured.

B. The Nature of the Harm

It might be tempting to think of a deepfake as being less harmful than a leaked private photo, as the image is fabricated. Nevertheless, research on image-based sexual abuse does not bear out this perspective. As noted by McGlynn and Rackley, there is a continuum of sexual abuse in relation to the taking, production, and distribution of sexual images without consent. In such

[2] Ian Goodfellow et al., Generative Adversarial Nets, 27 Advances Neural Info. Processing Sys. 2672 (2014).
[3] Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753, 1757–60 (2019).

ISSN: 2582-6433

a situation, the wrongdoing stems from a failure to govern how one presents oneself sexually.[4]. According to Citron, this interest can be called "sexual privacy" – the norms defining access to one's intimate life and body. According to her, a violation occurs even in cases where viewers know the image has been fabricated.

C. Gender Violence Enhanced Through Technology

Identifying sexual deepfakes as a matter related to gender justice lies in what I would call Three foundations. First, there is a gendered nature in regard to who is being attacked. Second, the damage inflicted by the attack discourages women and frightens them away from taking part in public discourse. Third, the international institutions consider technology-based violence in connection with violence against women. The CEDAW Committee acknowledges that gender-based violence can occur through technology. In addition, the Special Rapporteur on violence against women has categorized online violence as an extension of the other forms of violence that women encounter.[5] Though men and children can be affected too, the proposed measures in part seven take into account this type of targeting as well.

III. Theoretical Foundations: Consent, Privacy, and Dignity

A. Consent as Authority over Sexual Representation

Consent has shaped the law governing sexual offences in relation to physical acts for a considerable period of time. Image-based abuse extended the notion of consent because, for instance, consent to be photographed does not constitute consent to distribution of the photographs. However, deepfakes extend the notion further. There is no original context against which consent may be breached since there is no original image. As a result, consent must be conceived as an individual's ability to determine if and how his/her sexuality may be represented in a public space. In this regard, the crime of producing a sexual deepfake lies not in disclosure of some truth about the victim but in another person's writing of her sexuality. Hence, consent in this regard is highly context-bound and revocable; permission to produce a certain image for one occasion does not authorise using it for production of a different, synthetic one.

B. Privacy after K.S. Puttaswamy case

The nine judge bench in Puttaswamy recognized privacy as a fundamental right falling under

[4] Clare McGlynn & Erika Rackley, Image-Based Sexual Abuse, 37 Oxford J. Legal Stud. 534 (2017).
[5] Comm. on the Elimination of Discrimination Against Women, General Recommendation No. 35 concerning Gender-Based Violence Against Women, ¶ 20, U.N. Doc. CEDAW/C/GC/35 (July 26, 2017); Special Rapporteur on Violence Against Women, Its Causes and Consequences, Report addressing Online Violence Against Women and Girls from a Human Rights Perspective, U.N. Doc. A/HRC/38/47 (June 18, 2018).

ISSN: 2582-6433

Articles 14, 19 and 21. It protects one's body, informational autonomy and decision-making. It is a part of one's dignity[6]. The sexual deepfake is related to all three aspects – interfering with the bodily integrity in terms of representation, using a person's facial features as personal information without consent, and depriving her of control over her image. Previous judicial decisions support this interpretation. In Rajagopal, the court recognised a right to privacy. In Mardikar, the court recognised even a woman of loose morals has a right to privacy. Puttaswamy deals with the right to privacy against state action. However, when deepfake technology is used, it is private individuals that are doing it. Injunctions have been issued by the courts to aid this issue but there is not yet much development of the horizontal application of this right.

C. Dignity, Equality, and Paternalism

Dignity under Art. 21 and equality according to Arts. 14 and 15 are aspects related to gender justice. In the cases of Vishaka, equality and dignity formed the bases of an obligation for a work environment that was free from sexual harassment, and in Joseph Shine, adultery was invalidated partly due to the deprivation of autonomy for women. Based on these rulings, the law will best protect women by protecting their autonomy [7]and not by "modesty." Anuj Garg highlights the caution needed to avoid paternalistic measures which limit the freedom of women in the course of protecting them. [8]Suggestions for women to remove themselves from internet spaces are examples of such policies that must be rejected.

IV. The Indian Legal Framework

A. Bharatiya Nyaya Sanhita, 2023

Section 77 BNS (which replaces IPC S. 354C) is the offence of watching or capturing the image of a woman in the course of a private act or of disseminating such an image[9]. There has to be a real act and a real recording in order for the section to apply; a fabricated image doesn't really fit. The section is strictly construed. Section 79 (BNS equivalent of IPC S.509) provides that it shall be an offence to speak, make noises, gestures or display objects with the intention to outrage the modesty of any woman and to intrude upon her privacy.[10]. The privacy limb is very promising and Rupan Deol Bajaj goes on to define modesty in such a way as to encompass sexualised imagery. This section can be limited by intent and by the narrow definition of

[6] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
[7] Vishaka v. State of Rajasthan, (1997) 6 S.C.C. 241, (Joseph Shine v. Union of India, (2019) 3 S.C.C. 39.
[8] Anuj Garg v. Hotel Ass'n of India, (2008) 3 S.C.C. 1 (India).
[9] Bharatiya Nyaya Sanhita, 2023, S. 77, No. 45, Acts of Parliament, 2023.
[10] Id. S. 79

ISSN: 2582-6433

modesty.[11]. Defamation (S. 356), forgery of an electronic record with the intent to damage reputation (S. 336(3)), extortion (S. 308) and criminal intimidation (S. 351) will all apply in certain factual scenarios (e.g. sextortion), but none of them actually name the core wrong[12].

B. Information Technology Act, 2000

Section 66E deals with punishment for capturing, publishing or transmitting the image of a private area of any person without his/her consent.[13] It is gender-neutral, but an appellate court has not ruled on whether a computer-generated image is eligible. Sections 66C and 66D on identity theft and cheating by personation require dishonesty and cheating so are not ideal. In practice, the most work is done by sections 67 and 67A. Section 67A is for the sending or publishing of sexually explicit material electronically. It can lead to up to 5 years imprisonment and a fine of up to 10 lakh rupees for a first offence.[14]. These provisions work because they look at content, not provenance, but they treat the wrong as obscenity, a matter of community standards, not want of consent.[15]

C. Intermediary regulations and amendments in 2026

Section 79 of IT Act provides a safe harbour to intermediaries. In Shreya Singhal, the Supreme Court read down section 79(3)(b), so that rights of removal arise on a court order or a government notification.[16] Intermediaries must act quickly on complaints of intimate images (including artificially morphed images) under the 2021 Intermediary Rules."[17] Notified on 10 February 2026 and effective from 20 February 2026, the Amendment Rules, 2026, define "synthetically generated information", require prominent labeling and provenance metadata, and require intermediaries providing generative tools to take reasonable measures against unlawful synthetic content, which includes non-consensual intimate imagery and reducing the time to take down.[18] This is the most important legislative step taken so far, but it regulates the platforms after publication, not the person who created the image.

D. Digital Personal Data Protection Act, 2023

A face is personal data, and making a deepfake processes that data, so the consent-based DPDP Act might seem apt. But section 3(c)(i) exempts personal data processed by an individual for a

[11] Rupan Deol Bajaj v. K.P.S. Gill, (1995) 6 S.C.C. 194 (India).
[12] Bharatiya Nyaya Sanhita, 2023, S. 308, 336(3), 351, 356.
[13] Information Technology Act, 2000, S. 66E, No. 21, Acts of Parliament, 2000 (India).
[14] Id. S. 67, 67A.
[15] Aveek Sarkar v. State of W.B., (2014) 4 S.C.C. 257 (India) (applying a community standards test to obscenity).
[16] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b) (India).
[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026

ISSN: 2582-6433

personal or domestic purpose, which a private creator will readily claim.[19] The obligations under the Act are also largely on data fiduciaries and the remedies are through the Data Protection Board. This may involve contacting a commercial modification service.

E. Judicial reactions

The High Courts, particularly Delhi, have provided most of the effective protection. Public figures' personality-rights suits generated injunctions against AI misuse of likeness and voice[20]. More significant are suits by unpublicised women. The Delhi High Court granted an ad interim injunction against numerous websites and accounts distributing morphed and deepfake sexual content in Kamya Buch v. JIX5A, found that Google had de-indexed the identified URLs and ordered that the plaintiff's identity be kept from the public record.[21] One analysis found Delhi to be the main forum, followed by Bombay and Madras, with takedown orders rarely appealed. [22] The Madras High Court has also directed the Union to take down intimate pictures of a woman lawyer within a stipulated time, indicating that the approach is not confined to one bench or city. [23] These orders are a confirmation of the fact that courts read privacy and dignity into private disputes but they are interim, civil and individual require access to a High Court, a lawyer and time.

V. Critical Analysis: Gaps in the Law

- Offences grounded in reality - Section 77 BNS and on its text, section 66E are based on capture of something that happened. They may be stretched by the courts, but a victim should not have to rely on creative interpretation of a penal statute.
- Obscenity replaces consent - Sections 67 and 67A do not concern themselves with whether the person depicted consented or not, but whether the material is obscene or sexually explicit. It centers the viewer's sensibilities, invites debate over community standards, and treats a consensual explicit image and a non-consensual deepfake the same.
- The modesty lexicon - Section 79 retains the language of insulting modesty, which is part of an understanding of women's sexual integrity as honour and not as right, and which the later gender justice cases discussed in Part III depart from.

[19] Digital Personal Data Protection Act, 2023, S. 3(c)(i), No. 22, Parliament Acts 2023 (India).
[20] Anil Kapoor vs. Simply Life India, (2023) and Arijit Singh vs. Codible Ventures LLP (Bom.). HC July 26, 2024)
[21] Kamya Buch v. JIX5A (2025)
[22] Deepfakes and NCII in the High Courts, NALSAR Tech Law Forum (2025).
[23] Delhi HC orders X and Meta to take down AI-generated porn (2025).

ISSN: 2582-6433

- Creation and supply are unchanged - The provisions are directed at publication and transmission. The person who makes the image, the person who holds it to threaten release, and the developer who markets a nudification tool are only indirectly reached. The 2026 obligations on generative-tool providers are regulatory and depend on safe-harbour effects, not on criminal liability.
- The system relies on victim effort - Notice-and-takedown forces the victim to hunt down, report and chase every copy, while re-uploading is cheap. A further concern is the enforcement capacity: one report notes that funding under the Cyber Crime Prevention against Women and Children scheme fell sharply between 2017–18 and 2023–24 while cyber violence against women rose.
- Reputation and honour are the chief remedies. The question in defamation and related provisions is whether the victim's standing in society has suffered. That framing is too narrow, and quietly damaging. It places the injury in what others will think of her, which reinforces the social logic that makes these images so damaging to women in the first place, and it leaves the victim to prove harm to a reputation that the image may have damaged precisely because it was believed or because the community judged her for it. The consent-based framing spares us that burden because the wrong is done when the image is made or shared without permission, regardless of what anyone thinks.
- Freedom of expression and proportionality - Overly extensive criminalisation of synthetic media could inadvertently include satire and valid expression. Following Puttaswamy, any limitation must adhere to legality, pursue a legitimate aim, and be proportionate, while Shreya Singhal requires precise tailoring. Sexually explicit images of a recognisable individual, created or distributed without their consent, have minimal grounds for speech protection, thus, a carefully crafted, consent-focused offence can satisfy these criteria.

VI. Comparative Perspectives

Recently, various jurisdictions have enacted new laws. In the United Kingdom, the Online Safety Act 2023 introduced offences related to the distribution and threats of distributing intimate images, including those digitally altered, while the Data (Use and Access) Act 2025

ISSN: 2582-6433

established an offence for creating a supposed intimate image without consent.[24] In the United States, the TAKE IT DOWN Act of 2025 makes it illegal to publish non-consensual intimate imagery, including digital forgeries, and mandates that covered platforms remove such content within forty-eight hours of a legitimate request[25]. In 2024, Australia made it a crime to transmit sexually explicit deepfake material without consent.[26] Following incidents of deepfake abuse in schools and universities, South Korea expanded liability in 2024 to include the possession and viewing of such material.[27] The European Union's Directive 2024/1385 obliges Member States to criminalise the non-consensual distribution of intimate or manipulated material.[28]

Three key lessons emerge. Effective models characterize the offence based on lack of consent rather than obscenity, explicitly incorporating computer-generated images. These models are progressively addressing both the creation and distribution aspects. Additionally, they view criminal law and platform responsibilities as complementary. India's 2026 amendments embrace the platform-responsibility strategy but lack a corresponding offence definition.

VII. Recommendations

An offence focused on consent. It is recommended that Parliament amend the BNS to include an offence related to the creation, distribution, or threats to distribute sexually explicit synthetic media featuring an identifiable individual without their consent, with awareness or disregard for the absence of consent. The legislation should define "sexually explicit synthetic media" as any image, video, or audio that is generated or modified by computer to portray a real person engaged in a sexual act or in a state of undress. A person should be considered "identifiable" if they can be recognized from the media or any accompanying text. Consent must be specific to the intended use of the material and should be revocable. Obscenity should not be a component of this offence. The victim should be referred to using gender-neutral language, with more severe penalties for offences involving child victims or those committed for profit or through coercion.

- Responsibilities for tool creators and platforms - Developers or marketers of services primarily designed to produce non-consensual sexual images should be held accountable. Persistent failure to adhere to the 2026 obligations should result in tangible

[24] Online Safety Act 2023, c. 50, S. 188 (UK), inserting S. 66A, 66D into the Sexual Offences Act 2003; Data (Use and Access) Act 2025.
[25] TAKE IT DOWN Act, (2025).
[26] Criminal Code Amendment (Deepfake Sexual Material) Act 2024
[27] Act on Special Cases Concerning the Punishment of Sexual Crimes, as amended 2024.
[28] Directive 2024/1385, of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence, art. May 20, 2024 O. J. (L 2024/1385).

ISSN: 2582-6433

repercussions, including implementing safety-by-design measures like rejecting the processing of real individuals' photos for modification purposes.

- Victim-focused approach - Section 72 BNS, which safeguards the identities of victims of specific sexual crimes, ought to be applicable to the new offence. Courts should maintain the practice of keeping victims' information out of public records. Additionally, each State cyber unit should appoint a nodal officer responsible for issuing takedown requests, preserving evidence, and facilitating hash-matching to prevent re-uploads without the need for repeated reporting.
- The remedy in civil terms and compensation - The statutory tort of intrusion into sexual privacy, including injunctions, damages, and delivery of materials to the victim, would alleviate such victims the burden of having to prove their claim based on the infringement of personality rights or defamation, while compensation would be offered by the existing state victim compensation schemes.
- Capacity and protections - Specialized units and training for police and magistrates, legal assistance as well as complaint files in Indian languages are as important as any new regulation. Adequate exceptions for consent, lawful investigation, and bona fide reporting should be incorporated in the new crime, with an intention to keep separate the regulation of non-sexual political and parody deepfakes.

Conclusion

Sexual deepfakes show how outdated legal categories fail to match technology. Indian law still focuses on whether an image is obscene, whether modesty was violated, whether reputation was damaged or whether something was recorded. The real issue is whether someone took control of another person’s sexual self-representation without permission. High Courts have made some progress and the 2026 Amendment Rules take a step on the platform side. Yet criminal law has not yet named the harm. A defined offence based on consent backed by victim-centred procedures and clear duties for those who build and host such tools and proper enforcement resources would align the law with the person who is harmed. That is what gender justice demands. The constitutional language to do this already exists in the K.S. Puttaswamy, Vishaka and Joseph Shine case. All that remains is for Parliament to use it to address a harm that technology has made easy. That old laws were never meant to handle.