INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

HARMS OF DEEPFAKES BASED ON GENDER IN INDIA: A FEMINIST LEGAL ANALYSIS OF PRIVACY AND ONLINE HARASSMENT LAWS

AUTHORED BY - ADITHYA V S

I. Introduction

Advances in AI and machine learning have enabled the creation of what is popularly known as "deepfake" technology. This is technically synthetic media which includes various forms of images, videos or audio. This is the concept of portraying people doing or making these people say things that they never did.[1] These tools bring together the strengths of deep-learning architecture and media editing in order to make very convincing forgeries that come with questions of identity, consent and authenticity.[2] While deepfakes can give us many valuable products, they also provide many malicious outcomes such as sexualized, non-consensual and threatening contents that creates grave concerns for privacy and dignity.[3]

When it comes to the Indian context, the harms of deepfakes are mainly burden women. They are faced with higher vulnerabilities to non-consensual intimate imagery, blackmail or reputational harm.[4] The amplification of such gendered digital violence is compounded by issues such as unequal digital literacy, weak cyber policing and stigmatic societal norms against victims of sexualized image abuse.[5] With hundreds of millions of internet users in India, high digital penetration and low levels of awareness on the regulation of the cyberspace create the breeding ground for deepfake-enabled harassment.[6]

[1] What is Deepfake Technology? Definition from TechTarget, TechTarget (May 22, 2025), https://www.techtarget.com/whatis/definition/deepfake.
[2] What Is a Deepfake? Definition & Technology, Proofpoint (Apr. 2024), https://www.proofpoint.com/us/threat-reference/deepfake.
[3] Science & Tech Spotlight: Deepfakes, U.S. Gov't Accountability Office (GAO-20-379SP 2020).
[4] 'The chilling effect': how fear of 'nudify' apps and AI deepfakes is keeping Indian women off the internet, The Guardian (Nov. 5, 2025).
[5] Online Crimes Against Women in India: Deepfakes, Doxxing and Digital Abuse, CPPR (Oct. 23, 2025).
[6] Deepfakes in India: Legal Landscape, Judicial Responses & a Practical Playbook for Enforcement, National e-Govt Digital Service (Sept. 29, 2025).

The present research problem is that the Indian laws concerning privacy, online harassment, and sexualised digital harms are not yet fully adapted to the peculiar threats presented by AI-generated synthetic media.[7] Traditional legal frameworks focus on real image misuse, obscenity, or reputational harms but cannot foresee the layered challenges when a person's likeness is manipulated without consent through algorithmic means. It is in this context that this study, through the use of a feminist legal theory framework, examines how existing Indian legal instruments respond-or fail to respond-to gender-based deepfake harms and point to gaps in protection and redress. The methodology shall be purely secondary in nature: a doctrinal review of legislation, case law, and policy supported by feminist theoretical inputs on issues of autonomy, agency, and digital gendered violence.

II. Understanding Gendered Deepfake Harms

A. Nature of Deepfake Technology.

One the very base, deepfake technology is a system created by collaborating with artificial intelligence. The idea of this system is more generative in nature. It uses adversarial networks and diffusion models to either create or manipulate images and videos that depict individuals in situations they never took part in.[8] For example, one such method shows us that training a neural network on an immense corpus of images or video of a person and using this, this neural network is able to create a synthetic version of that person's face or voice and then this is easily used to make new content.[9] In contrast to earlier "morphing" techniques-which coarsely superimposed or blended faces-deepfake synthesis relies on learned representations of facial structure, lighting, and motion to create far more convincing and dynamic fakes.[10] Thus, from morphing to deepfake

[7] IT Act toothless against deepfakes? NCW seeks review of laggard laws as women face more AI-driven abuse, The Print (Nov. 18, 2025).
[8] What Are Deepfakes and How Are They Created?, IEEE Spectrum (May 6, 2019), https://spectrum.ieee.org/what-is-deepfake. ("To make a deepfake video … the creator would first train a neural network on many hours of real video footage of the person.")
[9] What Are Deepfakes and How Can We Detect Them?, The Turing Inst. (Apr. 2024), https://www.turing.ac.uk/blog/what-are-deepfakes-and-how-can-we-detect-them. ("There are two main groups of methods used to create image and video deepfakes: generative adversarial networks (GANs) and diffusion models.")
[10] Artificial Intelligence, Deepfakes, and the Uncertain Future of Truth, Brookings (Oct. 11, 2022), https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth.

synthesis, the leap lies in algorithmic automation and a considerably enhanced realism of the result, which makes detection substantially more difficult.[11]

B. Gendered Dimensions of Deepfake Abuse

Deepfakes is a powerful technology and using this there are many gender-based violence arising. This is particularly due to it being used to create non-consensual sexual imagery which is targeting women and other gender minorities.[12] Such content causes many harms such as reputational damage when a person is wrongly made to appear in sexual or intimate way in videos or photos. There is a particular social stigma and shame in communities where victims are stigmatised. Aside from that it also creates various forms of psychological harm, including anxiety, trauma and fear of exposure. Other than that this technology would be used for coercion or blackmail when perpetrators threaten to share deepfake content and real threatens to create problems concerning the personal safety of victims when captured footage is weaponised.[13] Other than this, certain already vulnerable populations such as Dalit women, Muslim women, queer and trans folks are at higher risk of deepfake abuse because the communities are already socially unacceptable because of their gender, caste, religion and sexuality.[14] These tools serve as an instrument of patriarchal control over women's images, bodies, and digital presence.

C. Feminist Legal Lens

From the point of view of feminist legal theory, the concept of deepfake abuse is not a new technological problem, it is a very well known patterns of gender-based violence but in a digital disguise.[15] Key concepts include bodily autonomy which is the right of people to control their

[11] How Deepfakes Are Made: AI Technology, Process & Detection Guide, RealityDefender (Oct. 2024), https://www.realitydefender.com/insights/how-deepfakes-are-made. ("At its core … training AI models on hundreds or thousands of images, videos or audio samples of an individual.")
[12] The Digital Dimension of Violence Against Women as…, Council of Europe (2022), https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae.
[13] Deepfakes in India: Legal Landscape, Judicial Responses & a Practical Playbook for Enforcement, NEGD (Sept. 29, 2025), https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/. ("Non-consensual sexual deepfakes disproportionately target women… they perpetuate gender-based violence … inflicting psychological trauma.")
[14] Akter, MS, The Emergence of AI-generated Deepfakes as a New Tool…, Feminists at Law, Vol. (2025) (exploring intersectional vulnerabilities).
[15] Technology-Facilitated Sexual Violence and Abuse in Low…, PMC (Oct. 2023), https://www.ncbi.nlm.nih.gov/articles/PMC10913330/.

image and representation. Secondly, digital consent, which is the right of individuals to control the use of their likeness or voice online. Finally, autonomy over one's digital identity.[16] The traditional legal approaches have focused on many concepts such as "obscenity" or "voyeurism," deepfakes challenge they very concepts of traditional legal frameworks by the implication of image creation, manipulation and dissemination without the victim's agency.[17] Ultimately, digital sexual harm through deepfakes reflects patriarchal patterns-whereby women's bodies and representations are controlled, circulated and punished in the digital world.[18]

III. Legal Framework in India

A. Constitutional Protections

The constitution of India along with the judiciary provides several protections regarding privacy, dignity and bodily integrity comes under the right to life and personal liberty under Article 21 of the Constitution of India.[19] The judiciary has assisted in landmark case of Justice K.S. Puttaswamy (Retd) v. Union of India (2017), it was held that the fundamental right to privacy is linked to Article 21 and Part III of the Constitution.[20] In this case it was stated that the privacy protects the freedom to make decisions about one's body and life. This means that the personal intimacy, sexual orientation and informational autonomy comes under this.[21] The peaking jurisprudence holds how digital personas and one's likeness online may also fall within the dignity area. However the direct protection from the synthetic-media harms remains absent.[22]

[16] Tech-Facilitated Gender-Based Violence (TFGBV), Equality Now, https://equalitynow.org/what-we-do/end-sexual-exploitation/tech-facilitated-gender-based-violence/.
[17] Deepfake Pornography: Examining the Impact on Women's…, Semanticscholar (2024) (highlighting gaps in laws like India's IT Act dealing with deepfakes).
[18] Based Violence Against Women in the Age of Social Media, IJFMR (2025) (digital harm as extension of gender-based violence).
[19] India Const. art. 21 ("No person shall be deprived of his life or personal liberty except according to procedure established by law.").
[20] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).
[21] Id. at paras. 119–121 (majority opinion) (explaining privacy protects "the freedom to make decisions about one's body and life").
[22] Id.; see also V. Bhandari et al., *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict* 4-5 (2017).

B. Information Technology Act, 2000

The main statute that takes care of cyber offences in India is the Information Technology Act, 2000 ("IT Act").[23]

Key provisions relevant to deepfake-style harms include

- Section 66E criminalises capture, publication or transmission of images of a private area of a person without consent;[24]
- Section 67, penalizing publication/transmission of "obscene" material in electronic form;[25]
- Section 67A punishes publishing/transmission of material containing sexually explicit acts.[26]
- Section 69A empowers the government to block access to information and content online.[27]

However, critics have stated that the IT Act's definitions revolving obscenity and requirement of "sexually explicit act" or "private image" is partial and does not fully regulate the idea of non-consensual synthetic media where publicly available images are manipulated rather than private captures.[28]

C. Bharatiya Nyaya Sanhita (BNSS)

The Bharatiya Nyaya Sanhita, 2023 contains several offences relevant to deepfake harms such as Section 73 (sexual harassment), Section 74 (voyeurism) and Section 75 (stalking). Aside from this, defamation provisions which comes under Sections 356–357, and Section 79 (insulting the modesty of a woman) may be applied when manipulated or synthetic imagery harms reputation, dignity or privacy. But still many of these provisions still rely on concepts such as "modesty," "offensive behaviour," or intention to insult and the legal framework revolves around misuse of real images. This makes it more difficult to prosecute cases involving fully synthetic or AI-generated deepfakes where no original image existed.

[23] Information Technology Act, 2000, No. 21 of 2000 (India).
[24] Id. § 66E (India) ("Whoever intentionally or knowingly captures, publishes or transmits the image of a private area of any person … without his or her consent…").
[25] Id. § 67 (India) ("Punishment for publishing or transmitting obscene material in electronic form").
[26] Id. § 67A (India) ("Punishment for publishing or transmitting electronically any material containing sexually explicit act").
[27] Id. § 69A (India) ("Power to issue directions for blocking for public access of any information through any computer resource").
[28] See, e.g., M. Srikant, *Bharatiya Laws Against Deepfake Cybercrime: Opportunities & Challenges*, VIF India (Apr. 28, 2025) (noting that obscenity-based definitions under the IT Act limit applicability to synthetic media).

D. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 came into force in August 2023 and it is used to regulate digital personal data processing in India. This will include consent based obligations for Data Fiduciaries.[29] All processing of digital personal data under the Act requires free, specific, informed and unambiguous consent.[30] The government has stated that "deepfakes using personal data without consent can attract penalties" under its area.[31] But there is still a shortcoming which is that the Act fails to clearly cover "synthetic data" or AI generated contents and removes the publicly available personal data from certain requirements, hence this will be leaving a gap in regulation of deepfakes generated from public imagery.[32]

E. Case Law

Currently there are no landmark Indian judgment focused on the concept of deepfakes, the courts have applied IT Act and IPC offences to morphed image and cyber harassment cases.[33] One of the best example of this is the cases that come under Section 67 of the IT Act, the courts have expressed its concern regarding the materials that must must display a "sexually explicit act" to attract the provision but this limits the application to many creative forms of deepfake misuse.[34] The lack of any jurisprudence solely on synthetic media would mean that the existing law remains untested in this context and the deepfakes continue to become exhibited within the grey zone of liability.[35]

IV. Feminist Critique of India's Laws

A. Substantive Gaps

Even though there is a heavy rise in synthetic media and non-consensual deepfake imagery there is no correct recognition under Indian law of "non-consensual deepfake pornography" or synthetic

[29] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
[30] Id. ch. II, § 5 (requiring free, specific informed consent for processing personal data).
[31] Press Information Bureau, *India Well-Equipped to Tackle Evolving Online Harms and Cyber Crimes*, (Aug. 2025) (noting that "deepfakes using personal data without consent can attract penalties" under data laws).
[32] See M. Srikant, supra note 10 (observing DPDP Act's failure to directly address synthetic-data or AI-generated likenesses).
[33] See Lawyered.in, *Cyber Sexual Harassment Against Women* (Mar. 2023) (explaining courts have applied IT Act and IPC to morphed image and cyber-harassment cases, though no specific deepfake jurisprudence).
[34] Lawctopus, *Legislative Challenges Revolving around Deepfake Technology* (Aug. 6, 2025) (noting courts under § 67 have required depiction of "sexually explicit act" and therefore many deepfakes evade liability).
[35] Id. (observing absence of any Indian judgment directly addressing synthetic media/deepfakes and liability remains untested).

sexual imagery as a proper offence.[36] The existing provisions under the Information Technology Act, 2000, the Indian Penal Code, 1860 and the Digital Personal Data Protection Act, 2023 assume the misuse of actual photographs or "private images" and not algorithmically generated content.[37] For instance, the IT Act punishes the capturing or transmitting images of a person's "private area" without consent under Section 66E but does not clearly extend to AI-generated content created from publicly available imagery.[38] A review of regulatory comments notes that synthetic images "fall outside definitions" that presupposes existing personal data or traditional image capture.[39] Recent feminist legal scholarship underscores how failing to codify abuses of synthetic media in the law leaves its victims unprotected in a rapidly changed technological environment.[40]

B. Patriarchal Language & Framing

A criticism shows that laws bear a strong influence of patriarchal, morality oriented language. Provisions like "modesty" or "insult to modesty" (IPC Section 509) and "obscene publication" (IT Act Section 67) place emphasis on protection of societal morality when compared to autonomy and dignity.[41] Feminist legal theorists argue that this framing it this way institutionalizes a protectionist rather than an agency centred model. Women are framed as objects who need significant protection instead of being agents or humans who can control their own image and representation.[42] Deepfake harms show an old pattern of gender-based control over women's bodies and images and the law's language shows strong signs of patriarchy by focusing on "community standards" of decency rather than consent and autonomy.[43]

[36] Siddharth Johar, *Articulating a Regulatory Approach to Deepfake Pornography in India*, NLS IJLT Blog (2023).
[37] M.M. Sharma, *Deepfake Pornography: Examining the Impact on Women's Lives*, 1 J. Sexuality & Gender L. 24 (2024).
[38] Id.
[39] Deepfakes in India: Legal Landscape, Judicial Responses & a Practical Playbook for Enforcement, NEGD Blog (Sept. 29, 2025).
[40] A. Ma'arif, *Social, Legal, and Ethical Implications of AI-Generated Image-based Violence*, Porn Stud. (2025).
[41] Shalu Nigam, *Beyond Modesty: Feminist Legal Theory on Women's Online Agency*, (forthcoming).
[42] Feminist legal analysis of digital harassment in India, Feminism in India (Nov. 1, 2025).
[43] CIGI, *Women Not Politicians Are Targeted Most Often by Deepfake Videos*, (Mar. 3, 2021) ("Deepfakes … exploit, humiliate and harass … through the age-old tactic of stripping women of their sexual autonomy.")

C. Consent and Agency

The right to "digital consent" which is the ability to decide whether one's image or voice is used online [44] Victims of non-consensual deepfake imagery face many procedural burdens in proving non-consent and intent and identifying the source. This often causes them to not report such cases and live with it.[45] Feminist critiques show how victim blaming discourage making it difficult to lead on with these cases as the proof lies with women. But even then, their credibility is doubted by the police are often supposed to apathy towards complaints.[46] Even when the deepfake technology has significantly improved the law remains fixated on direct photographic capture and this cannot account for algorithmic manipulation at a very complex level.[47] Women and gender minorities remain thus doubly disadvantaged first by the harm itself and then by the legal system which fails to recognize digital agency.

D. Platform Accountability

Social media, messaging apps and content hosting services exercise governance powers in the digital environment over the circulation of deepfakes.[48] As it currently stands under the IT Act, the safe harbor provisions protect the intermediaries from liability unless there has been a failure to act upon a takedown notice.[49] The feminist perspective indicates that any inaction or slow action by platforms has disproportionately harmed women: while private firms decide content governance, the legal framework offers scant affirmative accountability for gendered harms.[50] The most recent report on deepfakes flagged how slow-reacting platforms are to requests for takedowns and thus extend exposure and amplify harm.[51] This means the law leaves women open to risk without stringent platform accountability, including proactive detection, gender-sensitive policies, and transparent redress.

[44] Id.; see also Sharma, supra note 2.
[45] S. Johar, supra note 1.
[46] Feminism in India, supra note 7.
[47] Sharma, supra note 2.
[48] Id.; see also Johar, supra note 1.
[49] Id.
[50] Feminism in India, supra note 7.
[51] The Guardian, 'The chilling effect': How fear of 'nudify' apps and AI deepfakes is keeping Indian women off the internet (Nov. 5, 2025).

E. Intersectional Impact

Finally, an intersectional feminist critique emphasizes the fact that deepfake harms are not gender-neutral; they operate through intersections of gender, caste, religion, and sexuality.[52] In India, for instance, Dalit, Adivasi, Muslim, queer, and trans women are especially vulnerable to digital sexual violence, including deepfake abuse, because of structural discrimination and a lack of access to digital rights.[53] The fear of such harms has real behavioural consequences: Some women report self-censoring online activity out of fear of deepfake "nudify" apps or AI-based harassment.[54] The failure of the law to account for these layered vulnerabilities means protections for the most impacted groups are weakest. Feminist legal analysis underlines that to be gender-just, regulation must recognize the amplified risk faced by marginalised identities and adopt tailored safeguards.[55]

V. Comparative Insights

The different regulatory responses to the harms created by gendered deepfakes from other jurisdictions offer some important lessons for India. For example, under the Online Safety Act 2023 (UK), it has been made it a "priority offence" to share or threaten to share intimate images, including deepfakes, without consent and new offences are proposed to criminalise the creation of sexually explicit deepfakes.[56] These measures make non-consensual synthetic sexual content a crime and assign clear responsibilities to platforms to remove such content.[57]

In South Korea, lawmakers have taken aggressive steps. Recent a bill has been made which criminalizes viewing or possessing sexually explicit deepfakes with penalties as long as three years' imprisonment or fines of 30 million won.[58] This has shown recognition that synthetic-media harms extend beyond creation and distribution to consequences through circulation and

[52] Id.; see also Sharma, supra note 2.
[53] Feminism in India, supra note 7.
[54] Id.
[55] Ma'arif, supra note 5.
[56] Government crackdown on explicit deepfakes, UK GOV.UK (Jan. 7 2025), https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes.
[57] S. Moreno, Deepfakes and the Law: Why Britain needs stronger protections against technology-facilitated abuse, QMUL Law News (Jan. 24 2025).
[58] South Korea to criminalise watching or possessing sexually explicit deepfakes, Reuters (Sept. 26 2024).

consumption. The Korean approach recognises the high volume of deepfake sex offences and enforces many criminal liabilities even without profit motive.[59]

The EU's DSA and AI Act impose duties of care and transparency on the platforms.[60] Among other things, the DSA requires online officers to take measures to reduce the spread of manipulated content and label it as the same. The AI Act classifies "synthetic media" as a category that requires transparency measures and risk assessments.[61]

From these comparative frameworks these are the few lessons for India:

- Explicit criminalisation of non-consensual and synthetic sexual imagery instead of subsuming it under older obscenity or privacy statutes.
- Rapid takedown standards that make sure that the platforms are responsible for taking down labelled synthetic media within narrow timeframes.
- Stronger platform duties such as compulsory detection and labelling of synthetic media, subjects of disclosure and liability in case of non-compliance
- These reforms would be a step toward aligning India's legal framework with the technological realities of AI-driven gender-based digital violence.

VI. Recommendations for India

A. Legal Reforms

The creation, distribution or threat of non-consensual synthetic sexual imagery more commonly known as deepfakes, must be explicitly criminalised within India's legal system.[62] This shall take the shape of a distinct addition to the Information Technology Act, 2000, Indian Penal Code, 1860 or proposed Bharatiya Nyaya Sanhita, 2023.[63] 'Non-consensual synthetic sexual imagery' generated or manipulated through AI will be included in every such law for the first time.[64] Further,

[59] ADRN Issue Briefing: South Korea's Vulnerability to Deepfake Sex Crimes, East Asia Institute (Dec. 2024).
[60] Tackling deepfakes in European policy, EU Parliament (2021).
[61] Title: Deepfakes and the Indian legal framework: A call for specific legislation, Amicus Qriae (2025).
[62] Swanand Bhale, *Deepfake Laws in India: The Need for Legal Regulation in the AI Era*, SSRN (Feb. 1, 2025).
[63] Anish-adapted: See VIF India, "Bharatiya Laws Against Deepfake Cybercrime: Opportunities and Challenges", Apr. 28 2025.
[64] Anish-adapted: See VIF India, "Bharatiya Laws Against Deepfake Cybercrime: Opportunities and Challenges", Apr. 28 2025.

legislation should acknowledge individuals' rights over their digital identity and voice and it should be affording victims a clear claim to representation autonomy online.[65]

B. Regulatory Reforms

Regulatory measures need to supplement substantive law. First, mandating rapid takedown timelines-for instance, 24-48 hours after a validated complaint-by platforms reduces the duration of exposure and mitigates harm to victims.[66] Second, platforms should be required to adopt technical safeguards such as watermarking or provenance-tracking for AI-generated content and undergo independent transparency audits.[67] Recently, the Indian government proposed rules mandating visible labels covering at least 10% of surface-area for visual AI-content and requiring user declaration of AI-origin content.[68] These measures provide a starting point for regulation-but need to be calibrated with gender-harm contexts and victim rights.

C. Procedural Reforms

Procedural reforms become important to make sure that rights become accessible. The cyber-cells and law-enforcement units must be gender-sensitive, trained specifically in digital sexual harms and AI-enabled abuse.[69] Forensic processing of digital deepfakes should be streamlined, resourced and time-bound so that evidence is collected before further dissemination.[70]Victims must be given anonymity, protection from further victim-blaming, and specialist legal-aid services should be availed to be with the dynamics of AI-enabled gendered violence.[71]

D. Social and Educational Measures

Socio-educational testing beyond the law and regulation are needed. Digital literacy programs aimed at women especially in rural and semi-urban India, can help them understand the risks of image misuse, synthetic media and deepfakes.[72] Public awareness about AI-generated sexual harm

[65] Ibid.
[66] Asian Institute of Research, *Deepfake Technology in India and World: Foreboding and Forbidding*, (2025).
[67] Times of India, "Government plans tweaks in law to guard against deepfakes", (Sept. 2025).
[68] Reuters, "India proposes strict rules to label AI content citing growing risks", Oct. 22 2025.
[69] VIF India, supra note 2.
[70] Lawvs, "Deepfake Regulation vs. Free Speech: Should India criminalise AI-generated deepfakes under fundamental rights concerns?", Nov. 1 2025.
[71] Ibid.
[72] Asian Institute of Research, supra note 4.

should be raised as a form of gender-based violence. Safe-reporting channels and visibility for survivors can be created through collaboration between government, civil society, and platforms.[73] Finally, if India is to respond effectively to deepfake-enabled gender harms, is a rights-based multi-layered approach that adopts a combination of legal reform, regulatory duty, procedural accessed and social education. So long as the law does not explicitly define the offence, platforms do not comply with strict standards, enforcement remains unattuned, and communities are not empowered, the gendered harms of synthetic sexual imagery will continue to grow unchecked.

VII. Conclusion

In order to sum up everything that has been stated so far there is a largely applicable gendered dimension of digital harm in India which is non-consensual deepfakes which commonly target women and gender minorities and it causes reputational, psychological and privacy harms magnified by a lacking legal structure.[74] Recent research suggests that many Indian women are avoiding to post images or participating in online spaces out of fears of their images being manipulated.[75] The existing legal architecture in India is just a patchwork. While there are provisions under the Information Technology Act, 2000, Indian Penal Code, 1860 and the Digital Personal Data Protection Act, 2023 none are tailored for synthetic-media harms.[76] From a feminist legal perspective, means that structural gaps persist-laws are framed in terms of morality or obscenity rather than with regard to autonomy and the right to consent; platform accountability is weak; and intersectional vulnerabilities remain unaddressed.[77] A feminist legal framework requires a dignity-centred and consent-based approach with an intersectionally sensitive approach to deepfake regulation: one which views digital likeness as integral to bodily integrity, treats synthetic sexual imagery as a form of gender-based violence, and meaningfully protects women

[73] Ibid.
[74] Sarigama R. Nair, *The Emerging Threat: Deepfake and Women in India*, IJCRT Vol. 12 Issue 5 (May 2024). ("Deepfakes … put women in India at serious risk …")
[75] Vikram Kumar, 'The chilling effect': How fear of 'nudify' apps and AI deepfakes is keeping Indian women off the internet, The Guardian (Nov. 5 2025).
[76] Anu Maria Francis, *Online Crimes Against Women in India: Deepfakes, doxxing and digital abuse*, CPPR (Oct. 23 2025). ("While revenge porn, deepfakes … don't have standalone legal provisions in the law.")
[77] Beatriz Kira, *Deepfakes, the Weaponisation of AI Against Women and Possible Solutions*, Verfassungsblog (June 3 2024). ("Most AI-generated image-based sexual abuse targets women … existing systems are likely inadequate.")

and marginalised genders.[78] Given the speed with which AI is being taken up and the minimal barriers to the creation and dissemination of manipulated media, the urgency for reform cannot be overstated. Unless timely and nuanced legal, regulatory, and social interventions occur, the gendered harms caused by deepfakes will further undermine women's capability to participate freely and safely in India's digital society.

[78] Agnes E. Venema, *Deepfakes as a Security Issue: Why Gender Matters*, WIISGlobal (2023). ("Deepfakes … a gendered security issue … because the potential damage … can be immense.")

Bibliography

1. "Based Violence Against Women in the Age of Social Media," IJFMR (2025).
   India Const. art. 21.
2. "Deepfake Pornography: Examining the Impact on Women's…" SemanticScholar (2024).
3. "Deepfakes in India: Legal Landscape, Judicial Responses & a Practical Playbook for Enforcement," NEGD Blog (Sept. 29, 2025), https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/.
4. "IT Act toothless against deepfakes? NCW seeks review of laggard laws as women face more AI-driven abuse," *The Print* (Nov. 18, 2025).
5. "Tech-Facilitated Gender-Based Violence (TFGBV)," Equality Now, https://equalitynow.org/what-we-do/end-sexual-exploitation/tech-facilitated-gender-based-violence/.
6. "Technology-Facilitated Sexual Violence and Abuse in Low…" PMC (Oct. 2023), https://www.ncbi.nlm.nih.gov/articles/PMC10913330/.
7. "What Are Deepfakes and How Are They Created?," *IEEE Spectrum* (May 6, 2019), https://spectrum.ieee.org/what-is-deepfake. IPRI Institute+1
8. "What Are Deepfakes and How Can We Detect Them?," *The Turing Institute* (Apr. 2024), https://www.turing.ac.uk/blog/what-are-deepfakes-and-how-can-we-detect-them.
9. Anu Maria Francis, *Online Crimes Against Women in India: Deepfakes, Doxxing and Digital Abuse*, CPPR (Oct. 23, 2025).
10. Asian Institute of Research, *Deepfake Technology in India and World: Foreboding and Forbidding* (2025).
11. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
12. Indian Penal Code, 1860 (Act No. 45 of 1860) §§ 354A, 354C, 354D, 499–500, 509 (India).
13. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).

    Information Technology Act, 2000, No. 21 of 2000 (India).

14. Kinza Yasar, Nick Barney & Ivy Wigmore, *What Is Deepfake Technology? Definition from TechTarget* (May 22, 2025), https://www.techtarget.com/whatis/definition/deepfake. TechTarget
15. MS Akter, *The Emergence of AI-generated Deepfakes as a New Tool…*, Feminists at Law, Vol. (2025).
16. National e-Govt Digital Service (NEGD), *Deepfakes in India: Legal Landscape, Judicial Responses & a Practical Playbook for Enforcement* (Sept. 29, 2025), https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/.
17. Proofpoint, *What Is a Deepfake? Definition & Technology* (Apr. 2024), https://www.proofpoint.com/us/threat-reference/deepfake. prompt.tennessee.edu+1 U.S. Government Accountability Office (GAO), *Science & Tech Spotlight: Deepfakes* (GAO-20-379SP 2020).
18. Reuters, "India proposes strict rules to label AI content citing growing risks," (Oct. 22, 2025).
19. Swanand Bhale, *Deepfake Laws in India: The Need for Legal Regulation in the AI Era*, SSRN (Feb. 1, 2025).
20. Vikram Kumar, "'The chilling effect': how fear of 'nudify' apps and AI deepfakes is keeping Indian women off the internet," *The Guardian* (Nov. 5, 2025).