INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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

THE INVISIBLE HARM: A STRUCTURAL AND COMPARATIVE CRITIQUE OF INDIA'S LEGAL RESPONSE TO NON-CONSENSUAL DEEPFAKE PORNOGRAPHY

AUTHORED BY - SANJANA

ABSTRACT

The proliferation of deepfake technology has given rise to a distinctly modern form of sexual violence, namely the non-consensual generation and dissemination of synthetic pornographic imagery using a real person's likeness. While India witnessed its first major public reckoning with this phenomenon in late 2023, the legislative response has been, at best, reactive and, at worst, structurally inadequate. This paper undertakes a doctrinal critique of India's existing legal framework, primarily the Information Technology Act, 2000 as amended, alongside provisions of the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023. It argues that none of these instruments, individually or collectively, are capable of providing meaningful legal redress to victims of non-consensual deepfake pornography. The paper identifies three central structural failures: definitional inadequacy, an unworkable evidentiary burden, and the absence of proportionate remedies. Drawing on comparative frameworks from the United Kingdom, the United States, and the Republic of Korea, this paper argues that India's current approach reflects a legislature that has responded to the symptom without diagnosing the disease. It concludes with normative recommendations for a *sui generis* legislative intervention.

Keywords: deepfakes, non-consensual intimate imagery, IT Act 2000, digital sexual violence, intermediary liability

I. INTRODUCTION

In November 2023, a video purporting to show a prominent Indian actress in a compromising situation circulated rapidly across domestic social media platforms. The video was fabricated, being a product of deepfake technology that superimposed her face onto another person's body using artificial intelligence. Within days, similar videos targeting other public figures emerged. The Ministry of Electronics and Information Technology issued advisories to social media platforms, reminding them of their obligations under the IT Act and the Intermediary

ISSN: 2582-6433

Guidelines.[1] The government's response was swift in rhetoric but thin in legal substance. No new law was enacted. No charges were filed under any statute specifically addressing deepfake-based sexual harm. The incident faded from the news cycle, but the question it exposed did not: does India have a law capable of protecting people from this kind of harm?

India's IT Act 2000 remains the primary legislation governing digital offences, but it was drafted at a time when deepfakes were the stuff of science fiction. [2] The amendments of 2008 and the more recent regulatory activity in 2023 have not kept meaningful pace with technological reality. [3] Meanwhile, jurisdictions such as the United Kingdom, South Korea, and several US states have enacted targeted legislation specifically addressing synthetic media and non-consensual intimate imagery. India has not.

The analysis begins with a technical and conceptual grounding in what deepfakes are and why they present distinct legal challenges. The existing Indian legal framework, covering the IT Act, the BNS, and the DPDP Act, reveals three specific doctrinal failures. Foreign legislative responses from comparable jurisdictions offer instructive contrasts, leading to normative recommendations for reform.

The scope of analysis is limited to non-consensual deepfake pornography: the creation and/or distribution of sexually explicit synthetic media using a real person's likeness without their consent. Political deepfakes, synthetic audio fraud, and AI-generated content that does not involve identifiable real persons, while equally deserving of scholarly attention, fall outside the present inquiry.

II. DEEPFAKES AND THE ANATOMY OF DIGITAL SEXUAL VIOLENCE

2.1 What Is a Deepfake?

The term "deepfake" is a portmanteau of "deep learning" and "fake." It refers to synthetic media, typically video or images, generated using artificial intelligence and specifically a class of machine learning models known as Generative Adversarial Networks (GANs). A GAN

[1]Ministry of Electronics and Information Technology, *Advisory on Deepfakes* (November 2023), available at meity.gov.in.
[2]Information Technology Act, 2000, s 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023.
[3]Information Technology Act, 2000 (No 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008 (No 10 of 2009).

ISSN: 2582-6433

operates by training two neural networks in competition: one generates synthetic content and the other attempts to distinguish it from real content. Through successive iterations, the generative network produces increasingly convincing output that may be, to the untrained eye, indistinguishable from genuine footage.[4]

While deepfake technology has legitimate applications in film production, accessibility tools, and historical reconstruction, it has been weaponised overwhelmingly against women. A 2023 report by cybersecurity firm Home Security Heroes found that 98 per cent of all deepfake videos online were pornographic in nature and that 99 per cent of those targeted women.[5] This gendered dimension is not incidental. It reflects and reproduces existing patterns of technology-facilitated gender-based violence. The creators of such content are, in the vast majority of documented cases, motivated by a desire to degrade, humiliate, and silence.

2.2 The Nature and Extent of the Harm

Non-consensual deepfake pornography causes harm along multiple axes. At the individual level, victims report severe psychological trauma comparable in intensity, if not in character, to that experienced by survivors of physical sexual assault.[6] The Cyber Civil Rights Initiative's research consistently documents experiences of post-traumatic stress, depression, social withdrawal, and professional abandonment among victims.[7]

The harm is compounded by a distinctive feature of synthetic imagery, which is that the fabricated nature of the content does not diminish the reputational damage. A viewer who does not know, or does not care, that a video is synthetically generated may treat it as authentic. In a legal context, this creates a paradox: the very argument that might seem to reduce the harm is also the argument that makes existing legal frameworks inapplicable, since existing law covers real images and not fabricated ones.[8]

There is also a silencing effect that extends beyond the individual victim. Several empirical studies have documented victims withdrawing from public life and abandoning professional ambitions following the creation of deepfake content about them.[9] For public figures and aspirant public voices, particularly women in politics, journalism, and entertainment, this

[4]Bobby Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 *California Law Review* 1753, 1758.
[5]Home Security Heroes, "2023 State of Deepfakes Report" (2023), p 4, available at homesecurityheroes.com.
[6]Cyber Civil Rights Initiative, "NCII and the Law: A Survey of US and International Responses" (2023), p 12.
[7]Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 3-4.
[8]Cyber Civil Rights Initiative (n 7) 14-16.
[9]Mary Anne Franks, "Unwilling Avatars: Idealism and Discrimination in Cyberspace" (2011) 20 *Columbia Journal of Gender and Law* 224, 241.

ISSN: 2582-6433

represents a structural threat to democratic participation that goes beyond personal injury.

The harm is further characterised by its permanence and viral potential. Unlike a physical assault, a deepfake video can be copied, reuploaded, and redistributed across jurisdictions indefinitely. The practical impossibility of complete erasure means that the harm continues to accrue long after any legal proceeding has concluded, rendering conventional remedies such as criminal conviction and damages structurally incomplete.[10]

2.3 Why Legal Systems Struggle: Three Foundational Tensions

Before turning to the specific inadequacies of India's statutory framework, it is necessary to identify three foundational tensions between the nature of deepfake harm and the organising assumptions of existing legal systems. These tensions are not incidental features of the regulatory landscape. They are structural, and any legislative response that does not consciously address them will reproduce the same failures in a new form. Together, they explain why deepfake pornography is not simply an old harm in a new medium but a genuinely novel category of wrong that demands genuinely novel legal thinking.

The first tension is categorical, and it arises at the level of legal classification itself. Existing law governing harmful speech and imagery was built on a foundational assumption: that the content under scrutiny bears some relationship, however distorted, to an underlying reality. Defamation law asks whether a statement is false. Obscenity law asks whether material is offensive. Privacy law asks whether information was disclosed without consent. In each case, the legal inquiry begins with something real, either a real statement, a real image, or real personal information. Deepfakes disrupt this assumption entirely. They are not distortions of reality. They are fabrications that are designed to be indistinguishable from it. A deepfake video is not, in the legal sense, a false statement about a person. It is a fabricated depiction that mimics authentic visual evidence. The distinction is not merely semantic. It has direct consequences for how each element of an offence or cause of action must be formulated, and for the kind of evidence a victim must adduce to establish the wrong.

The second tension is jurisdictional, and it operates not between nations but between legal domains. Non-consensual deepfake pornography simultaneously engages at least four bodies of law: privacy law, because it involves the appropriation of a person's biometric likeness without consent; criminal law, because it inflicts deliberate harm of a sexual nature; intellectual property law, because the generated image uses aspects of a person's identity as raw material;

[10]Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn" (2014) 49 *Wake Forest Law Review* 345, 362.

ISSN: 2582-6433

and intermediary liability law, because platforms host and distribute the content. Each of these bodies of law offers a partial account of what has gone wrong, and none offers a complete one. A victim who pursues relief through all available channels must navigate courts and tribunals with different procedural requirements, different standards of proof, and different remedial powers. The cognitive and financial burden of this fragmented litigation landscape falls entirely on the person who has already been harmed. This jurisdictional incoherence is not a feature of deepfake law specifically. It is the product of a legal system that has accumulated responses to individual harms without ever developing a unified framework for technology-facilitated sexual violence.[11]

The third tension is temporal, and it may be the most consequential of the three. Law is inherently retrospective: it classifies and responds to harms that have already been identified, theorised, and litigated. Technology is inherently prospective, and the pace at which AI-based synthetic media tools have developed has consistently outrun the pace at which legislatures have been able to respond. The drafters of the Information Technology Act 2000 could not have anticipated a world in which a convincing fabricated video of any person could be generated in minutes using freely available software. The amendments of 2008 arrived before deepfakes existed as a practical phenomenon. The regulatory activity of 2023 acknowledged the problem but stopped short of addressing it legislatively. The result is a legal system that is perpetually catching up, deploying provisions designed for different harms in the hope that they will stretch to cover the new one.

These three tensions, categorical, jurisdictional, and temporal, are not independent. A legislature that does not define the harm clearly will produce provisions that sit uneasily alongside existing law and will already be outdated by the time they are enacted. The inadequacies of India's current framework are not the product of legislative carelessness or mere oversight. They are the product of attempting to address a genuinely novel harm through legal instruments that were designed for a different world.

III. THE EXISTING INDIAN LEGAL FRAMEWORK

3.1 The Information Technology Act, 2000

The IT Act remains the cornerstone of India's response to digital offences. Several provisions are potentially applicable to deepfake pornography, though none were designed with it in mind. Section 66E penalises the violation of privacy through the capture, publication, or transmission

[11]Chesney and Citron (n 5) 1772-73.

ISSN: 2582-6433

of a person's image in a mass transmittable medium without their consent.[12] The provision was clearly modelled on voyeurism statutes and addresses the non-consensual capture or sharing of real intimate images. It makes no reference to synthetic or AI-generated imagery. Whether a deepfake constitutes an "image" within the meaning of Section 66E is an open and unresolved question. The ordinary meaning of "image" could encompass synthetic imagery, but the interpretive context of the provision, which is concerned with the unauthorised capture of a real person's physical state, suggests it was not so intended.[13] No Indian court has definitively resolved this interpretive question.

Section 67 penalises the publication or transmission of obscene material in electronic form, while Section 67A extends this to sexually explicit material.[14] These provisions are content-based and would, on their face, apply to deepfake pornography irrespective of whether the content depicts a real or synthetic person. However, they are focused on the nature of the content rather than on the identity of the victim or the non-consensual use of their likeness. The specific wrong in non-consensual deepfake pornography is not merely that explicit content exists online. It is that a real person's identity and physical likeness have been appropriated for that content without their consent. Sections 67 and 67A do not capture this harm.

Sections 66C and 66D, dealing with identity theft and cheating by personation respectively, offer another avenue of analysis.[15] One might argue that using another person's biometric likeness to create a deepfake constitutes a form of identity theft. However, these provisions require that the accused use identity information "dishonestly or fraudulently," thereby importing a commercial or deceptive intent that may not be present in cases where the perpetrator's motivation is purely to harm or humiliate the victim. More fundamentally, the primary wrong in deepfake pornography is the sexual exploitation of a person's likeness and not the theft of their identity as such. The distinction carries material consequences for the elements of the offence and the appropriate sentencing framework.

The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 introduced the word "deepfake" into the Indian regulatory vocabulary for the first time, requiring intermediaries to take down content that misrepresents or manipulates the likeness of a real person.[16] This is a meaningful step forward. However, the Rules operate through the

[12]Information Technology Act, 2000, s 66E.
[13]Nandita Saikia, "Non-Consensual Intimate Imagery in India: Legal Lacunae and the Case for Reform" (2022) 7 *NALSAR Law Review* 88, 97.
[14]Information Technology Act, 2000, s 67.
[15]Information Technology Act, 2000, ss 66C and 66D.
[16]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, r 3(1)(b)(xi).

ISSN: 2582-6433

intermediary liability framework rather than creating direct criminal liability for the creator of deepfake content. They place primary obligations on platforms and not on perpetrators, and their enforcement depends on victim-initiated complaints, a model that, for reasons explored in Part IV, imposes an unreasonable burden on those who have already been harmed.

3.2 The Bharatiya Nyaya Sanhita, 2023

The BNS replaced the Indian Penal Code in 2023. Section 79, broadly corresponding to the former Section 354C of the IPC, addresses voyeurism and the dissemination of intimate images without consent.[17] Like the IT Act provisions discussed above, this section was drafted with reference to real intimate imagery, and its application to synthetic content is uncertain. Section 74 on sexual harassment and Section 75 on cyber-stalking may offer supplementary relief in particular factual scenarios, but neither addresses the core wrong, which is the fabrication of a person's sexual likeness without their consent.[18] [19]

There is no provision in the BNS that creates criminal liability specifically for the creation of synthetic intimate imagery. This is not an interpretive ambiguity. It is a straightforward legislative gap.

3.3 The Digital Personal Data Protection Act, 2023

The DPDP Act, a long-awaited development in India's data governance landscape, establishes a consent-based framework for the processing of "personal data," which includes biometric data.[20] [21] A deepfake is, in one sense, a product of biometric data processing: the AI model is trained on images of the victim's face, which constitute biometric information under any reasonable definition.

However, the DPDP Act's framework is concerned with data processing and consent to processing, and not with the harmful outputs of that processing. Even if one could establish that training an AI model on a person's images without consent violates the DPDP Act, itself a contestable proposition given the Act's broad carve-outs, the Act does not provide victims with the specific remedies they require, namely rapid content takedown, compensation for sexual and reputational harm, and criminal accountability for the creator.

The DPDP Act's enforcement mechanism operates through the Data Protection Board, which

[17]Information Technology Act, 2000, s 79.
[18]Bharatiya Nyaya Sanhita, 2023, s 79 (voyeurism).
[19]Bharatiya Nyaya Sanhita, 2023, ss 74 and 75.
[20]Digital Personal Data Protection Act, 2023 (No 22 of 2023).
[21]Digital Personal Data Protection Act, 2023, s 2(t) (definition of "personal data").

ISSN: 2582-6433

is not a court and lacks the remedial power that deepfake victims need.[22] Its penalty framework is calibrated for corporate data processors and not for individual actors engaged in targeted sexual harm. The Act, as it stands, offers victims no direct or practical path to relief.

IV. STRUCTURAL FAILURES OF THE EXISTING FRAMEWORK

4.1 Definitional Inadequacy

The most fundamental failure of India's existing legal framework is definitional. None of the provisions discussed above define "deepfake," "synthetic media," or "AI-generated content." This is not a technical complaint that can be dismissed as pedantry. Definitions determine the scope of liability, the elements that a prosecutor or claimant must establish, and the categories of harm that the law formally recognises.

The absence of a definition creates interpretive uncertainty at every stage of the legal process. A police officer receiving a complaint about deepfake content must determine under which provision, if any, to register an FIR. A prosecutor must frame the charge. A court must determine whether the conduct falls within the ambit of the section. At each stage, definitional ambiguity creates opportunities for the harm to fall through the cracks and, crucially, it creates opportunities for accused persons and their counsel to argue that the conduct is simply not addressed by any existing law.

This is not a hypothetical concern. Advocates working with survivors of technology-facilitated gender-based violence in India have consistently reported that police officers decline to register FIRs in deepfake cases on the ground that they are uncertain which provision applies. The Cyber Peace Foundation has documented multiple instances of deepfake victims being turned away at police stations or being advised to file under provisions that bear only a tangential relationship to the actual harm suffered.[23] The definitional vacuum in the law produces a practical vacuum in enforcement.

The 2023 Amendment Rules, as noted, use the word "deepfake" but do not define it, and they are directed at intermediaries rather than creators.[24] The definitional gap remains precisely where the primary wrong, being the act of creation, occurs.

[22]Digital Personal Data Protection Act, 2023, s 28 (establishment of Data Protection Board).
[23]Cyber Peace Foundation, "Deepfakes in India: Mapping the Harm and the Legal Vacuum" (2023), p 8.
[24]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, r 3(1)(b)(xi).

ISSN: 2582-6433

4.2 Evidentiary Burden and Investigative Infrastructure

Even where an applicable provision can be identified, the evidentiary burden on a victim of deepfake pornography is, in practice, prohibitive for the majority of complainants. The problem operates at two levels: the formal standard of proof and the practical investigative capacity to meet it.

To establish a case under any of the provisions discussed above, a victim must identify and link the accused to the creation or distribution of the content. In a typical deepfake case, the perpetrator operates anonymously through pseudonymous social media accounts, VPNs, and often through servers located outside India. Attribution requires forensic digital investigation of a kind that demands both legal authority and technical capability that most district-level police forces do not currently possess. India has no nationally standardised protocol for the investigation of AI-generated sexual harm, and the Cyber Crime Coordination Centre, while an improvement on preceding ad hoc arrangements, does not yet have the deepfake-specific forensic toolkit that effective investigation requires.

The intermediary liability safe harbour under Section 79 of the IT Act compounds this problem.[25] Platforms are incentivised, and indeed legally required, to remove content once notified. However, they are not required to assist in identifying the creator. The result is that content may be removed while the perpetrator faces no legal consequence. This asymmetry is particularly acute in deepfake cases, where the harm is ongoing because the content can be re-uploaded, and where the perpetrator is likely to target other victims if not apprehended.

The criminal standard of proof, being proof beyond reasonable doubt, is both correct in principle and demanding in practice. The investigative infrastructure required to meet that standard in a deepfake case, including cross-border mutual legal assistance, forensic AI attribution analysis, and real-time platform cooperation, is not systematically available in India.[26] This creates a structural asymmetry: technologically sophisticated wrongdoers can exploit the evidentiary gap while victims bear the full cost of the legal system's limitations.

4.3 Inadequacy of Remedies

The remedies available under the existing framework are inadequate in three distinct respects: they are too slow for the harm they address, insufficiently compensatory relative to the damage caused, and incapable of addressing the continuing and distributed nature of the harm.

[25]Information Technology Act, 2000, s 79(3); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r 4.
[26]Chesney and Citron (n 5) 1788.

ISSN: 2582-6433

Speed matters disproportionately in deepfake cases. The harm, comprising reputational damage, psychological trauma, and professional disruption, intensifies with every additional hour the content remains accessible. The legal system's ordinary timelines, from FIR to investigation to prosecution to adjudication, are measured in months and years. Meanwhile, a deepfake video can achieve tens of thousands of views within hours of being uploaded. There is no provision in India's current legal framework equivalent to an emergency civil injunction specifically designed for digital sexual harm. While civil courts possess the inherent jurisdiction to grant injunctive relief, the procedural obstacles to obtaining emergency orders against anonymous defendants operating through foreign platforms are, in practice, considerable.

The compensatory framework under Sections 43 and 43A of the IT Act was designed for data breaches and unauthorised access and not for sexual harm.[27] The quantum of civil damages available under these provisions does not reflect the actual and documented harm caused by non-consensual deepfake pornography, which includes severe psychological trauma, loss of professional opportunities, ongoing monitoring and removal costs, and long-term reputational damage that persists even after content is taken down.

None of the existing remedies address the continuing nature of deepfake harm. Once created and disseminated, a synthetic video can be archived, re-uploaded, and redistributed indefinitely. A criminal conviction addresses the past wrong but does not neutralise the ongoing harm. There is no provision in Indian law that compels the destruction of the underlying AI model, the deletion of biometric training data, or the creation of a hash-based database that platforms can use to prevent reuploads. These forward-looking, technical remedies are increasingly discussed in other jurisdictions and are entirely absent from the Indian legal arsenal.

V. COMPARATIVE ANALYSIS: LESSONS FROM ABROAD

5.1 The United Kingdom

The United Kingdom has moved most rapidly of any common law jurisdiction to address non-consensual deepfake pornography through dedicated legislation. The Online Safety Act 2023 introduced a specific offence of sharing intimate deepfakes without consent, explicitly extending the non-consensual intimate imagery framework to cover synthetically generated

[27]Information Technology Act, 2000, ss 43 and 43A.

ISSN: 2582-6433

content.[2829] This represented a conscious recognition that the earlier provisions addressing non-consensual real intimate imagery were technologically obsolete.

The Criminal Justice Act 2025 went further still by criminalising the creation of intimate deepfake images without consent, regardless of whether they are disseminated.[30] This legislative choice deserves emphasis because it represents a fundamentally different understanding of where the wrong lies. Under Indian law, the gravamen of any applicable offence is the distribution of harmful content. The UK Parliament recognised that the harm begins at creation: the making of such an image is itself a violation of the victim's dignity and autonomy, and the victim's injury is not contingent on whether anyone else ever sees the content.[31] The mere existence of the image constitutes an ongoing threat to the victim, and the law should reflect that reality.

Three features of the UK approach are directly instructive for India. The legislation is targeted, defining the offence with specificity by reference to both the synthetic nature of the content and the absence of consent, rather than relying on generic obscenity provisions. It is victim-centred, framing the offence around non-consent rather than content type. It is also forward-looking in its drafting, being consciously technology-neutral in the sense that it covers any electronically generated intimate imagery without limiting the offence to specific technical methods that might be rendered obsolete by future developments.

5.2 The United States

The United States' response has been characterised by the constitutional imperatives of its federal system, resulting in a patchwork of state legislation rather than an immediate unified federal framework, though federal action has now occurred.

California was among the first states to legislate, with AB 602 creating a civil cause of action for victims of deepfake pornography.[32] The significance of this approach lies in its accessibility: a civil cause of action operates at a lower evidentiary standard than a criminal prosecution and provides victims with a direct route to compensation without dependence on prosecutorial discretion. This is particularly important in cases where criminal investigation is unlikely to succeed due to anonymous perpetrators or jurisdictional complexity.

[28]Home Security Heroes (n 6) 7.
[29]Online Safety Act 2023 (UK), s 188.
[30]Criminal Justice Act 2025 (UK), Pt IV.
[31]Chesney and Citron (n 5) 1795, discussing the normative significance of creation as distinct from distribution in the context of synthetic sexual harm.
[32]California AB 602 (2019), codified at California Civil Code s 1708.86.

ISSN: 2582-6433

The DEFIANCE Act, enacted at the federal level in 2024, marked a watershed in US federal law.[33] It created a federal civil cause of action for non-consensual intimate deepfakes and was drafted with explicit attention to technological evolution. Its definitions are framed in terms of the harm and the absence of consent rather than in terms of specific technical processes, a drafting choice that avoids the obsolescence that has plagued earlier digital legislation.

The US experience also offers a cautionary lesson. Several early state statutes were drafted with stringent *mens rea* requirements, demanding proof that the accused specifically intended to cause distress to the victim. This proved, in practice, an undue burden: perpetrators of deepfake pornography can readily argue that their motivation was personal gratification rather than the intentional distress of the specific victim.[34] For India, the lesson is clear: intent-focused requirements should be avoided. The focus of the offence should be on the act and the absence of consent and not on the subjective purpose of the accused.

5.3 The Republic of Korea

South Korea has enacted arguably the most comprehensive legal framework for synthetic sexual harm of any Asian jurisdiction, and its experience is particularly instructive for India because both countries faced analogous catalysing events, namely the widespread targeting of female public figures through AI-generated sexual content, and because Korea's legislative response evolved in direct response to demonstrated inadequacies in an earlier statutory framework.

The Act on Special Cases Concerning the Punishment of Sexual Crimes was amended in 2020 to explicitly prohibit the creation, distribution, and possession of "edited, synthesized, or processed" sexual imagery of identifiable real persons without their consent.[35] Critically, the Korean law criminalises creation as a standalone offence, independent of distribution. Penalties for creation are substantial, and the law was subsequently further strengthened in 2023 following a wave of school-based deepfake incidents.

The institutional mechanism is equally notable. The Korea Communications Standards Commission was given specific statutory authority to order the removal of deepfake content, with legal obligations on platforms to comply within twenty-four hours of a notice.[36] This

[33]DEFIANCE Act 2024, Pub L No 118-214.
[34]Internet and Mobile Association of India, "AI and Synthetic Media: A Policy Framework for India" (2023), p 19 (noting the risk of over-broad *mens rea* requirements in early US state statutes).
[35]Act on Special Cases Concerning the Punishment of Sexual Crimes (Republic of Korea), as amended by Act No 17264 (2020) and Act No 19888 (2023).
[36]Korea Communications Standards Commission, Annual Report on Harmful Content Regulation (2023), pp 22-25.

ISSN: 2582-6433

administrative fast-track removal mechanism operates independently of the criminal process and provides a route to content removal that does not depend on the pace of police investigation or judicial process. It is, in effect, a dedicated emergency removal order for digital sexual harm, which is precisely the kind of mechanism that Indian law currently lacks.

The Korean experience demonstrates that legislative gaps in this area can be remedied through targeted reform and that such reform is achievable within a short timeframe when there is political recognition that the existing framework is failing victims. India has that recognition, as the ministerial advisories and public statements of 2023 demonstrate. What is lacking is the legislative follow-through.

5.4 The European Union

The EU's approach operates at a level of regulatory architecture above the specific problem of deepfake pornography, but it is nonetheless instructive for the direction of India's legislative development. The AI Act, adopted in 2024, classifies certain uses of AI as requiring specific disclosures and, in high-risk categories, conformity assessments.[37] Its relevance to deepfake pornography is indirect but not negligible: by imposing traceability requirements on AI-generated content, the AI Act creates an evidentiary infrastructure that could assist in attribution in sexual harm cases.

The GDPR has been deployed in several EU member states as a tool for seeking emergency injunctive relief against platforms hosting deepfake content, on the basis that generating and distributing such content constitutes unauthorised processing of biometric data.[38] This approach has achieved mixed results, since GDPR enforcement mechanisms were not designed for real-time content removal, but it has demonstrated that data protection frameworks can be repurposed for sexual harm cases in the absence of specific legislation. India's DPDP Act, in its current form, is not capable of serving this function for the reasons discussed in Part III. A targeted amendment could, however, potentially equip the Data Protection Board with emergency removal powers for deepfake content, serving a complementary function alongside dedicated criminal legislation.

[37]Artificial Intelligence Act, Regulation (EU) 2024/1689, Art 50 (transparency obligations for AI-generated content).

[38]General Data Protection Regulation, Regulation (EU) 2016/679, Arts 9 and 17.

ISSN: 2582-6433

VI. RECOMMENDATIONS

The comparative analysis above reveals a clear convergence in the direction of legislative reform across jurisdictions: targeted, victim-centred legislation that criminalises both creation and distribution of non-consensual deepfake pornography, accompanied by fast-track administrative removal mechanisms and accessible civil remedies. The following recommendations are advanced with the recognition that legislative reform is not, on its own, sufficient. Enforcement capacity, judicial training, and accessible legal aid are equally critical. However, the absence of adequate legislation is the most fundamental and most immediately addressable problem.

First: India requires a dedicated legislative provision, ideally a standalone chapter within the BNS or a specific amendment to the IT Act, that explicitly criminalises the creation and distribution of non-consensual synthetic intimate imagery. The provision must define its terms with sufficient precision to provide clear guidance to investigators and prosecutors while remaining technology-neutral enough to accommodate future developments. The definition of covered content should focus on the harm, being the depiction of an identifiable real person in sexual content without their consent, rather than on the specific technical method of generation. Second: The *mens rea* requirement should be anchored to non-consent and not to intent to harm. An accused person who creates a deepfake of a real person without their consent should not be able to avoid liability by arguing that their purpose was personal gratification rather than the deliberate distress of the victim. Knowledge that the content depicts a real person and that consent has not been obtained should be sufficient to establish the mental element of the offence.[39] This standard is consistent with the approach of the UK's Criminal Justice Act 2025 and avoids the enforcement failures documented in early US state legislation.[40]

Third: A fast-track administrative content removal mechanism, modelled on the Korean Communications Standards Commission approach, should be established. This mechanism should operate independently of the criminal process and should impose legally binding obligations on intermediaries to remove flagged deepfake content within twenty-four to forty-eight hours of receiving notice. The mechanism should also require platforms to implement hash-based detection systems to prevent the re-upload of previously removed content.

[39]UNESCO, "Governance of Deepfakes: A Global Survey of Legislative Responses" (2024), pp 34-36.
[40]Criminal Justice Act 2025 (UK), s 191 (knowledge-based standard for non-consensual intimate image offences).

ISSN: 2582-6433

Fourth: A standalone civil cause of action for victims should be created, with a rebuttable presumption of harm upon proof of creation and/or distribution. This removes the burden on victims of individually proving the quantum of psychological and reputational damage in civil proceedings, a process that is both difficult and retraumatising. The civil remedy should be available alongside, and not as a substitute for, criminal prosecution.

Fifth: The DPDP Act should be amended to explicitly address the use of a person's biometric data, including images, for the training of AI models that generate intimate synthetic imagery. Victims should have an enforceable right to demand the deletion not only of generated content but of the underlying training data, and the Data Protection Board should be empowered to issue emergency orders to this effect.

VII. CONCLUSION

The harm caused by non-consensual deepfake pornography is real, severe, and disproportionately borne by women. It is also growing. The technology that enables it has become dramatically more accessible over the course of the past three years. What once required considerable computational resources and technical expertise can now be accomplished by anyone with a smartphone and a downloaded application. The gap between the legal framework available to victims and the technological capabilities available to those who would harm them is widening, not narrowing.

India's existing framework, being a patchwork of provisions drafted for different harms and applied with interpretive uncertainty by investigative mechanisms inadequate to the task, fails victims at every stage of the legal process. It fails them at the definitional level, because no existing provision clearly covers the specific harm of synthetic intimate imagery. It fails them at the evidentiary level, because the infrastructure required to attribute and prosecute deepfake offences is not systematically available. And it fails them at the remedial level, because no existing remedy is fast enough, comprehensive enough, or forward-looking enough to address the continuing and distributed nature of deepfake harm.

The governments of the United Kingdom, South Korea, and the United States have recognised these failures and have moved, imperfectly but demonstrably, to address them through targeted legislation. India has not. The 2023 ministerial advisories and the Amendment Rules are acknowledgments that the problem exists. They are not solutions. A solution requires

ISSN: 2582-6433

legislation that names the harm, defines the wrong with clarity, creates liability for both creators and distributors, provides victims with accessible and timely remedies, and equips enforcement agencies with the tools they need to investigate effectively.

The question is not whether India will need such legislation. The technology exists, the harm is occurring at scale, and the legal vacuum is documented. The question is how many victims will be failed by the current framework before that legislation arrives.

BIBLIOGRAPHY

I. Statutes and Regulations

Indian

Information Technology Act, 2000 (No 21 of 2000)

Information Technology (Amendment) Act, 2008 (No 10 of 2009)

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended 2023

Digital Personal Data Protection Act, 2023 (No 22 of 2023)

Bharatiya Nyaya Sanhita, 2023

Foreign

Online Safety Act 2023 (UK)

Criminal Justice Act 2025 (UK)

Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act 2024 (US), Pub L No 118-214

California Civil Code s 1708.86 (AB 602, 2019) (US)

Act on Special Cases Concerning the Punishment of Sexual Crimes (Republic of Korea), as amended 2020 (Act No 17264) and 2023 (Act No 19888)

Artificial Intelligence Act, Regulation (EU) 2024/1689

General Data Protection Regulation, Regulation (EU) 2016/679

II. Cases

Shreya Singhal v *Union of India* (2015) 5 SCC 1

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

ISSN: 2582-6433

III. Books and Articles

Chesney B and Citron DK, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 *California Law Review* 1753

Citron DK, *Hate Crimes in Cyberspace* (Harvard University Press, 2014)

Citron DK and Franks MA, "Criminalizing Revenge Porn" (2014) 49 *Wake Forest Law Review* 345

Franks MA, "Unwilling Avatars: Idealism and Discrimination in Cyberspace" (2011) 20 *Columbia Journal of Gender and Law* 224

Franks MA, *The Cult of the Constitution* (Oxford University Press, 2019)

Saikia N, "Non-Consensual Intimate Imagery in India: Legal Lacunae and the Case for Reform" (2022) 7 *NALSAR Law Review* 88

IV. Reports and Policy Documents

Cyber Civil Rights Initiative, "NCII and the Law: A Survey of US and International Responses" (2023)

Cyber Peace Foundation, "Deepfakes in India: Mapping the Harm and the Legal Vacuum" (2023)

Home Security Heroes, "2023 State of Deepfakes Report" (2023)

Internet and Mobile Association of India, "AI and Synthetic Media: A Policy Framework for India" (2023)

Korea Communications Standards Commission, Annual Report on Harmful Content Regulation (2023)

Ministry of Electronics and Information Technology, Advisory on Deepfakes (November 2023)

UNESCO, "Governance of Deepfakes: A Global Survey of Legislative Responses" (2024)