REVENGE PORN VS. DEEPFAKE PORN: IS INDIAN LAW EQUIPPED FOR THE DIGITAL SHIFT?

Ravneet Kaur*

ABSTRACT

The rapid evolution of digital technology has transformed the nature of online sexual exploitation, giving rise to complex forms such as deepfake pornography alongside the already prevalent issue of revenge porn. While revenge porn involves the non-consensual dissemination of intimate images, deepfake pornography employs artificial intelligence to fabricate realistic but entirely manipulated explicit content. This article examines whether the existing Indian Legal Framework- primarily under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023- adequately addresses these emerging harms. It argues that although current provisions penalise obscenity, voyeurism and defamation, they fail to explicitly recognise the unique and invasive nature of deepfake content. The article further explores the challenges in establishing consent, intent and identity in such cases. It concludes by emphasising the urgent need for specific legislative intervention to bridge the legal lacuna and ensure effective protection of victims in the digital age. By distinguishing consent in traditional and AI- generated contexts, the article underscores the inadequacy of existing legal remedies.

Keywords: Revenge Porn, Deepfake Pornography, Consent, Digital Privacy, Bharatiya Nyaya Sanhita.

INTRODUCTION

The unprecedented growth of digital technology and social media platforms has fundamentally reshaped the contours of privacy, autonomy and personal relationships. While these advancements have facilitated communication and expression, they have simultaneously

*BA LLB (HONS.), FOURTH YEAR, UNIVERSITY INSTITUTE OF LEGAL STUDIES, PANJAB UNIVERSITY.

created new avenues for exploitation and abuse. Among the most concerning manifestations of such misuse is the phenomenon of non- consensual dissemination of intimate content, commonly referred to as revenge pornography. This practice not only infringes upon an individual's privacy but also results in severe emotional, psychological and reputation harm.[1]

In recent years, the emergence of artificial intelligence- driven technologies has further complicated this landscape through the proliferation of deepfake pornography. Unlike traditional revenge porn, which involves the sharing of real images or videos, deepfake pornography enables the creation of highly realistic yet entirely fabricated explicit content by superimposing an individual's likeness onto another person's body. The accessibility of such technology has significantly lowered the barriers to creating such content, thereby amplifying the scale and impact of digital harm.

The gravity of these violations must be understood in light of constitutional protections afforded under Indian law. The recognition of the right to privacy as a fundamental right under Article 21[2] has elevated concerns surrounding informational autonomy and bodily integrity. However, the rapid pace of technological advancement has outstripped the development of corresponding legal safeguards, resulting in a regulatory vacuum.

Although existing statutory provisions under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, provide certain remedies against obscenity, voyeurism and privacy violations, they were not designed to address the complexities introduced by artificial intelligence- generated content. This raises critical questions regarding the adequacy, scope and adaptability of the current legal framework in tackling emerging forms of digital exploitation.

REVENGE PORN AND DEEPFAKE PORN: A CONCEPTUAL SHIFT

Revenge pornography traditionally involves the unauthorised dissemination of intimate images, often by a former partner, with the intent to harass or humiliate. In contrast, deepfake pornography represents a paradigm shift, as it involves fabricated content generated using artificial intelligence tools, often requiring only a single image of the victim.[3] Revenge

[1] Abhay Jain, 'Deepfakes and Misinformation: Legal Remedies and Legislative Gaps' (2025) Indian Journal of Law
[2] Constitution of India, Article 21
[3] Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn" (2014) 49 Wake Forest Law review 345

pornography and deepfake pornography, although often grouped under the broader category of non- consensual intimate imagery (NCII), represent two fundamentally distinct yet interconnected forms of digital harm.

However, the emergence of deepfake technology has transformed the very nature of such violations. Deepfake pornography does not rely on pre- existing intimate material; instead, it uses artificial intelligence to fabricate highly realistic explicit content by superimposing an individual's likeness onto another person's body.[4] This marks a significant conceptual shift- from misuse of shared intimacy to the manufacture of false intimacy.

Indian courts have increasingly begun to recognise this shift. In Kamya Buch v. JIX5A & Ors, the Delhi High Court acknowledged that AI- generated explicit content constitutes a "patent breach" of privacy and dignity under Article 21, even though the material was fabricated rather than real.[5] The Court's approach indicates a move toward recognising harm based not merely on the authenticity of the content but on its impact on the individual's dignity and reputation.

The conceptual shift from revenge porn to deepfake pornography thus reflects a broader transformation, like digital harm, from violations of privacy to violations of identity itself. While revenge porn undermines confidentiality and trust, deepfake pornography challenges the very notion of authenticity and personal autonomy in the digital sphere.

Consequently, this evolution necessitates a corresponding shift in legal understanding. The law must go beyond traditional notions of consent and obscenity to address the emerging realities of AI- driven identity manipulation. Without such adaptation, existing legal frameworks risk becoming inadequate in addressing the profound and evolving harms posed by deepfake technology.

EXISTING LEGAL FRAMEWORK AND JUDICIAL APPROACH

The Indian Legal framework governing non- consensual intimate imagery and deepfake pornography remains largely fragmented and indirect, relying on a combination of statutory provisions and judicial interpretation.[6] In the absence of a dedicated legislation addressing

[4] Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy' (2019) 107 California Law Review 1753.
[5] Kamya Buch v. JIX5A & Ors ,Delhi High Court, 2025
[6] 'Deepfake Laws in India: Punishment and Complaint' (JuriGram)

deepfakes, courts and enforcement agencies have been compelled to adapt existing laws to emerging technological harms.

At the statutory level, the Information Technology Act, 2000, provides the primary legal basis for addressing online offences. Section 66C criminalises identity theft, which may be invoked in cases involving unauthorised use of a person's likeness in deepfake content.[7] Section 66D penalises cheating by personation through electronic means.[8] Section 66E addresses the violation of privacy through the capture or transmission of private images.[9] Additionally, Sections 67 and 67A criminalise the publication and transmission of obscene and sexually explicit material in electronic form.[10]

Parallel, the Bharatiya Nyaya Sanhita, 2023 (BNS) offers remedies through provisions relating to obscenity, defamation and offences against the modesty of a woman.[11] These provisions, however, were not designed with technologically manipulated content in mind, thereby limiting their applicability in complex deepfake scenarios.

The judiciary has played a pivotal role in expanding the scope of these provisions through constitutional interpretation. In Justice K.S. Puttaswamy v. Union of India, the Supreme Court unequivocally recognised the right to privacy as a fundamental right under Article 21, encompassing informational privacy and bodily autonomy.[12] This judgment serves as the constitutional foundation for addressing both revenge porn and deepfake pornography. Further, in Shreya Singhal v. Union of India, the court emphasised the importance of balancing freedom of speech with reasonable restrictions, particularly in the digital space.[13] The ruling also clarified intermediary liability, which is crucial in ensuring the timely removal of harmful online content.

Indian courts have recently begun to address deepfake-related harms more directly. In Anil Kapoor v. Simply Life India, the Delhi High Court granted a broad injunction against the unauthorised use of the actor's name, image, voice and likeness through artificial intelligence tools, thereby recognising the legal significance of personality rights in the digital age.[14]

[7] Information Technology Act, 2000, s 66C
[8] Information Technology Act, 2000, s 66D
[9] Information Technology Act, 2000, s 66E
[10] Information Technology Act, 2000, s 67 and s 67A
[11] Bharatiya Nyaya Sanhita 2023, s 74- 79, 356
[12] Justice K.S.Puttaswamy v Union of India (2017) 10 SCC 1
[13] Shreya Singhal v Union of India (2015) 5 SCC 1
[14] Anil Kapoor v Simply Life India & Ors CS (COMM) 608/2023

Similarly, in Kamya Buch v. JIX5A & Ors, the court ordered the immediate takedown of AI-generated explicit content, holding that such material constitutes a clear violation of privacy and dignity.

Additionally, in Amitabh Bachchan v. Rajat Negi, the Delhi High Court issued a John Doe order restraining unknown persons from misusing the actor's personality attributes, including through deepfake technology.[15] Such orders reflect the judiciary's willingness to adopt preventive measures in response to evolving digital threats.

Despite these developments, the reliance on judicial creativity highlights a significant legislative gap. Courts are effectively stretching traditional legal doctrines- such as defamation, obscenity and privacy- to accommodate new technological realities. While this approach ensures interim protection, it lacks the certainty and uniformity that a dedicated statutory framework would provide.

Therefore, although the Indian judiciary has demonstrated commendable adaptability in addressing deepfake- related harms, the absence of explicit legislative recognition continues to undermine the effectiveness and consistency of legal remedies in this domain.

CHALLENGES IN REGULATING DEEPFAKE PORNOGRAPHY

The regulation of deepfake pornography in India is not merely hindered by technological complexity but is fundamentally constrained by doctrinal limitations within existing legal frameworks. Unlike traditional forms of cyber offences, deepfake pornography disrupts the foundational legal assumptions on which current laws are built, thereby exposing structural inadequacies rather than mere enforcement gaps.

Doctrinal inadequacy of existing legal categories: Existing provisions relating to obscenity, defamation and privacy are premised on real content. Deepfake pornography, however, involves fabricated material that causes real harm, creating a doctrinal mismatch.[16] As a result, such cases often fall between legal categories, leading to fragmented and inconsistent application.

[15] Amitabh Bachchan v Rajat Negi & Ors, 2022
[16] Robert Chesney and Danielle Citron, 'Deepfakes: A Looming Challenge for Privacy' (2019) 107 California Law Review 1753

Rethinking consent in the digital age: Deepfakes challenge the traditional understanding of consent. While revenge porn focuses on unauthorised dissemination, deepfakes involve the absence of consent at the stage of creation itself. This necessitates recognition of identity- based consent, a concept not yet fully developed in Indian jurisprudence despite the constitutional recognition of privacy in Justice K.S. Puttaswamy v. Union of India.

Evidentiary and epistemic concerns: The admissibility standards laid down in Anvar P.V. v. P.K. Basheer create procedural hurdles in proving deepfake cases.[17] More significantly, deepfakes undermine the reliability of digital evidence itself, raising broader concerns about establishing authenticity in judicial proceedings.

Enforcement and anonymity: The anonymous and rapidly disseminated nature of deepfake content limits the effectiveness of traditional enforcement tools. Although courts have issued John Doe orders, as seen in Amitabh Bachchan v. Rajat Negi, such measures remain largely reactive. The transnational nature of digital platforms further complicates enforcement.

Intermediary Liability and Regulatory Gaps: The existing framework under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, relies on a reactive model of content removal.[18] In the context of deepfakes, where harm is immediate and widespread, this approach is inadequate and highlights the need for more proactive regulatory mechanisms.

These challenges demonstrate that deepfake pornography exposes a deeper issue of conceptual obsolescence within the law. Addressing it requires not merely stricter enforcement, but a rethinking of legal principles to account for identity, consent and technological manipulation in the digital age.

EMERGING TRENDS AND NEED FOR REFORM

Recent developments in India indicate a gradual but significant shift in the legal and judicial approach toward deepfake- related harms. Courts, particularly the Delhi High Court, have increasingly recognised that the misuse of artificial intelligence to replicate an individual's image, voice, or likeness constitutes a serious infringement of privacy, dignity and personality

[17] Anvar PV v PK Basheer (2014) 10 SCC 473
[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

rights.[19] In cases such as Anil Kapoor v. Simply Life India and Kamya Buch v. JIX5A & Ors, courts have granted broad injunctive relief, including takedown orders and restrictions on the use of digital likeness, thereby acknowledging the unique and evolving nature of such violations.

This judicial trend reflects an important transition from viewing such acts merely as instances of obscenity or defamation to recognising them as violations of identity and autonomy. However, this evolution remains largely judge- led and reactive, relying heavily on constitutional interpretation and equitable remedies rather than a clearly defined statutory framework. While the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India provides a strong constitutional foundation, its application to deepfake technology remains in a lack of doctrinal clarity and uniformity.

Another notable trend is the growing emphasis on intermediary responsibility in addressing the spread of deepfake content. Regulatory frameworks such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence obligations on platforms, including the requirement to remove unlawful content upon receiving actual knowledge. However, the existing notice- and- takedown model is inherently reactive and often fails to provide timely relief in cases where content spreads rapidly across multiple platforms. The viral and replicable nature of deepfakes demands a more proactive approach, including automated detection mechanisms and stricter compliance standards for intermediaries.

Furthermore, recent policy discussions and legal scholarship highlight the need to reconceptualise traditional legal doctrines to address the challenges posed by artificial intelligence. Deepfake pornography exposes the limitations of existing categories such as obscenity, defamation and privacy, which are not equipped to deal with the fabrication of identity itself. This has led to increasing calls for the recognition of digital identity rights and identity- based consent, which would grant individuals greater control over the use and manipulation of their likeness in digital spaces.[20]

[19] Anil Kapoor v Simply Life India & Ors CS (COMM), 608/2023 (Delhi High Court); Kamya Buch v JIX5A & Ors (Delhi High Court, 2025)
[20] 'Deepfakes, Consent and Law: Catching Up with AI Reality' (Vidhikarya, 25 November 2025) https://www.vidhikarya.com/legal-blog/deepfakes-consent-legal-challenges-in-ai-era accessed 19 March 2026

From a reform perspective, the issue is not merely one of strengthening penalties but of developing a coherent and technology- responsive legal framework. Such a framework must address both preventive and remedial aspects of deepfake harms. Preventively, it should impose obligations on platforms and developers to detect and limit the creation and dissemination of harmful synthetic media. Remedially, it must ensure swift and effective mechanisms for content removal, victim compensation, and legal redressal.

Key areas for reform include:

- The introduction of a clear statutory definition of deepfake and synthetic media.
- Explicit criminalisation of non- consensual AI- generated explicit content.
- Recognition and protection of digital personality and identity rights.
- Imposition of proactive due diligence obligations on intermediaries.
- Establishment of fast- track mechanisms for takedown and grievance redressal.

In conclusion, while India is witnessing an emerging awareness of the risks posed by deepfake technology, the current legal response remains fragmented and reactive. The increasing reliance on judicial innovation underscores the urgent need for comprehensive legislative intervention. A shift towards a principle- based and future- oriented regulatory framework is essential to ensure that the law evolves in tandem with technological advancements and continues to effectively safeguard individual dignity and autonomy in the digital age.

CONCLUSION

Revenge pornography and deepfake pornography represent two evolving dimensions of digital harm, both rooted in violations of dignity, privacy and autonomy. While Indian courts have shown commendable adaptability in addressing such issues through constitutional principles and existing legal provisions, the absence of a dedicated legislative framework continues to hinder effective enforcement. Scholarly analysis has consistently highlighted the legislative vacuum in India's response to deepfake pornography.[21] The challenge, therefore, is not merely to extend existing laws but to fundamentally rethink the legal approach to digital harms. Deepfake pornography necessitates the recognition of new legal constructs, including digital identity rights and identity-based consent, which reflect the realities of an AI- driven

[21] Subha Venkatraman, 'The Legal Vacuum in Regulating Non- consensual AI generated Pornography in India' (2025) IJRLM

ecosystem. Without such conceptual evolution, the law risks remaining anchored in outdated paradigms incapable of addressing technologically sophisticated violations.

Ultimately, safeguarding individual dignity in the digital age requires a shift from reactive adjudication to proactive and technology- responsive regulation. A comprehensive legal framework that integrates constitutional values with technological awareness is essential not only to address present harms but also to anticipate future challenges. In the absence of such reform, the gap between law and technology will continue to widen, leaving individuals increasingly vulnerable in an era defined by digital replication and manipulation.