DEEPFAKE PORNOGRAPHY AND CRIMINAL LAW OF INDIA: THE CRISES OF LEGAL CLASSIFICATION

Saloni Shashank Patil & Satya Prakash Mishra, Chhatrapati Shivaji Maharaj University, Panvel, Navi Mumbai, Maharashtra, India

ABSTRACT

Major strides have been taken by artificial intelligence (AI) in recent years, and it has consequently assumed a pivotal role in the production of synthetic media. "Deepfake pornography" is a by-product of such contemporary AI technologies. It brings forth profound legal difficulties that present-day criminal law struggles to regulate properly, as it is developed without an individual's voluntary consent. The article persuasively contends that pre-existing legal categories are deficient in adequately covering identity-based injuries or injuries stemming from non-consent. Thus, the article posits that "deepfake pornography" underscores how strongly established criminal law categories fail to achieve their intended goal. Their application is ill-suited to the novel forms of harm that are spawned by pioneering technologies. The article evaluates how the relevant sections of the Indian Penal Code and the Information Technology Act, 2000, tackle damage by relying on notions such as obscenity, defamation, and impersonation. This article delves into the specific legal complexities that criminal law in India encounters, providing concrete examples and case studies to illustrate the challenges of incorporating deepfake pornography into pre-existing legal categories. Varied consequences and divergent reactions across institutions are a result of ambiguously articulated definitions, making the enforcement vague when those who are affected bring forward concerns. Thus, it contends that erroneous categorisation may lead to setbacks in the process, ultimately leaving those impacted with insufficient remedies. The final point made is that tailored mechanisms are imperative to effectively construe and implement present-day legal regulations, bearing in mind the new modalities of digital sexual abuse. This will enable the law to competently manage deepfake-associated sexual exploitation.

1. An Overview

Due to the development of artificial intelligence, the human capacity to manipulate images and videos digitally has dramatically increased. What's more, it is executed effortlessly with an unprecedented level of accuracy. This pioneering development has the most alarming implication in the form of an upsurge of "deepfake pornography". It encompasses unauthorised digital insertion of a person's likeness into highly sexualised content, and that too without the individual's voluntary consent.[1] Although the deepfake content commonly looks indistinguishable from real, verifiable images when viewed, it is spurious. Thus, it ultimately becomes the chief reason for devastating individual as well as societal repercussions.[2]

Cases related to such deepfake pornographic content are the underlying reason for triggering and intensifying public discontent. However, no conclusive legal action has been initiated so far. Laws that are intended to regulate offences related to deepfake porn were formally adopted in the period prior to the advent of realistic synthetic sexual images.[3] Consequently, there are conceptual limitations under present-day Indian law on "how to classify deepfake pornography." Multiple setbacks keep appearing when a case of deepfake pornographic content is brought before the judiciary. Revenge porn constitutes a separate phenomenon from deepfake pornography. The chief factor highlighting their difference is that deepfake pornography does not necessitate verifiable nude pictures. The actual extent of damage suffered and who bears accountability are the two major issues before legal professionals.[4]

This article explores the thorny dilemmas Indian criminal law grapples with in attempting to categorise deepfake pornography. It transcends primary considerations of punishment or enacting an entirely novel legislation. It evaluates why prevailing legal notions cannot adequately cope with digitally manipulated sexual abuse. It posits that it's a critical requirement to establish more unambiguous criteria for categorising these offences. In order to shield individuals who could be impacted, clear, unambiguous criteria are imperative. Additionally,

[1] Danielle Keats Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1760–63 (2019).
[2] HENRY AJDER, ET AL., THE STATE OF DEEPFAKES: LANDSCAPE, THREATS, AND IMPACT (2019), https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.
[3] LAW COMM'N OF INDIA, REPORT NO. 272: ASSESSMENT OF STATUTORY FRAMEWORKS RELATING TO WOMEN, 38–40 (2017).
[4] Taylor Percival James, *Not Her Fault: AI Deepfakes, Nonconsensual Pornography, and Federal Law's Current Failure to Protect Victims*, 50 BYU L. REV. 1159, 1167-1168 (2025).

it's vital to confirm that the legislation that is put into practice is without any discrepancies.

2. Developing a Conceptual Understanding of Deepfake Pornography

To put it succinctly, artificial intelligence is utilised for developing deepfake pornography. To achieve verisimilitude for pornographic content, deepfake pornography is designed to produce or change someone's visual or auditory identity unbeknownst to the person involved.[5] In contrast to image-based sexual abuse that relies on real, verifiable material, deepfake pornography produces fabricated but believable sexual imagery or videos.[6] The chief detriment stems from assaulting an individual's identity and tarnishing their reputation, as opposed to unveiling what truly transpired.[7] Those who are impacted are subjected to recurrent exposure to public opprobrium and encounter psychological strain.[8] They risk losing agency over their digital persona. Data on digital platforms may propagate swiftly and stay discoverable over longer durations, resulting in commonly intensifying such detrimental impacts.[9]

By virtue of its synthetic composition, deepfake pornography critiques assumptions grounded in prevailing legal architecture. Most notably, those which are founded on the idea that behaviour is observable, it is physically generated through overt conduct, corroborated by direct witness testimony, or verified through tangible exhibits. Hence, it is constructive to assign deepfake pornography to a category of manifestation of internet-facilitated sexual harm. Also, it is indispensable to ascertain legal responses or reforms, such as the establishment of precise and enhanced legal categories, which are crucial to meaningfully address deepfake-facilitated sexual exploitation.

3. India's Extant Legal Framework

At the present juncture, an unambiguous and precise statutory criminal provision targeting deepfake pornography is not present in India.[10] Also, many present-day laws were written bearing in mind older types of online abuse. Thus, it forces victims to fall back on a fragmented array of crimes in the Indian Penal Code and the Information Technology Act, 2000.[11] Key

[5] Citron & Chesney**,** *supra* note 1, at 1760-1763.
[6] Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1898–1901 (2019).
[7] WOODROW HARTZOG, THE INVENTION OF PRIVACY, 65–68 (2018).
[8] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 353–55 (2014).
[9] Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (1997).
[10] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1, ¶¶ 83–87 (India).
[11] The Indian Penal Code, No. 45, Acts of Parliament, 1860, §§ 292, 354C, 499–500 (India);

transgressions encompass obscenity, impersonation, defamation, voyeurism, as well as the dissemination of pornographic content digitally.[12] Obscenity offences quite often prioritise enforcing societal norms instead of questions of consent or misused identities.[13] Defamation law rests on whether a person's reputation was truly impaired.[14] Voyeurism also presumes that someone was truly watched.[15] Notwithstanding, these stipulations provide certain restricted forms of redress only as they weren't developed considering artificial sexual content in view.[16] Hence, they typically offer only minimal and circuitous redress when they are applied to misfeasance of deepfakes. This array of clauses limits the exercise of authority to specific actions.

Unequivocal and straightforward directives are conspicuously missing pertaining to the proper classification of deepfake pornography. Thus, ambiguity is triggered at the phase of law enforcement as the responsibility to determine the legal classification of the offence is imputed to law enforcement personnel. As they are left with no choice, law enforcement personnel have to select from interconnected forms across a spectrum. As a result, a lack of standardisation and inconsistency across regions is seen as a common feature of FIR filing procedures. There exists heterogeneity in methods of prosecution, too. Prosecution practices vary across cases and regions. Such a disjointed framework fosters unpredictability when filing complaints, investigating, and prosecuting cases. These ingrained premises are ill-suited when the material is a synthetic visual in place of a verifiable event. Hence, it commonly prompts victims to step away before the proceedings conclude.[17]

4. Dilemmas of Legal Classification

A serious and persistent problem is presented before the criminal law of India in the form of deepfake pornography. This issue can be evidenced by specific cases and statistics that underscore the growing threat and implications of deepfake-facilitated sexual exploitation. Deepfake pornography produces a doctored sexual image or video tied to an identifiable person, rather than sharing a verifiable, intimate image.[18] This harm can be sexual, damaging

The Information Technology Act, No. 21, Acts of Parliament, 2000, §§ 66D, 67, 67A (India).
[12] Avnish Bajaj v. State (NCT of Delhi), (2008) 150 DLT 769 (India).
[13] Ranjit D. Udeshi v. State of Maharashtra, AIR 1965 S.C. 881 (India).
[14] Subramanian Swamy v. Union of India, (2016) 7 S.C.C. 221, ¶¶ 148–150 (India).
[15] The Indian Penal Code, No. 45, Acts of Parliament, 1860, § 354C (India).
[16] LAW COMM'N OF INDIA, *supra* note 3, at 45–48.
[17] NAT'L CRIME RECORDS BUREAU, CRIME IN INDIA 2022, 162–64 (2023).
[18] Citron & Franks, *supra* note 8, at 353–55.

to reputation, and tied to identity. However, such harm is hard to fit into present-day offence categories, as it is created through synthetic media. This uncertainty has real practical ramifications as it results, quite often, in ambivalence or hesitation when registering the FIR, application of wrong legal provisions, and evidence being framed poorly.[19] It has frequently been observed in cases that have entered the public record that law enforcement personnel rely significantly on the extant provisions of the Indian Penal Code and Information Technology Act for tackling deepfake-facilitated sexually explicit or defamatory content.[20] Hence, the absence of a specific statutory category can be evinced from such cases. The Supreme Court has forewarned that when legal categories are vague or poorly defined, they can lead to arbitrary enforcement. This risk is especially sharp for offences that involve technology, as the Court rightly noted in *Shreya Singhal v. Union of India*.[21]

4.1 Articulating the Core Wrong

Given that deepfake pornography produces or circulates synthetic intimate content and depicts identifiable individuals unbeknownst to them, it is considered intrinsically problematic. It ends up leading to profound sexual distress as the identity of individuals is abused. Decisional autonomy, along with informational privacy, was reaffirmed by the Supreme Court in *K.S. Puttaswamy v. Union of India*. It accentuated the fact that non-consensual alteration of the digital likeness of an individual involves dignity and identity rights that extend beyond reputational harm.[22] The courts of India treat unconsented sharing of sensitive visuals as a grave form of cyber sexual abuse, as documented in *State of West Bengal v. Animesh Boxi*.[23]

4.2 Obscenity and the Limitations of Moral-Based Approaches

Under the Information Technology Act and the Indian Penal Code, deepfake pornography is predominantly addressed as obscene material due to its overt sexual content.[24] This is treated as such because instead of centring on the injury inflicted by unauthorised sexual persona distortion, obscenity provisions centre on societal morality. Characterising this as an "obscenity

[19] LAW COMM'N OF INDIA, *supra* note 3, at 45–47.
[20] Yunus Dar, *The curious case of Babydoll Archi: The AI illusion that trapped millions*, BUSINESS STANDARD, (July 16, 2025), https://www.business-standard.com/social-viral/the-curious-case-of-babydoll-archi-the-ai-illusion-that-trapped-millions-125071600807_1.html.
[21] *Shreya Singhal*, 5 S.C.C. at ¶¶ 83–87.
[22] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[23] State of W. Bengal v. Animesh Boxi, 2018 S.C.C. OnLine Cal 448 (India).
[24] The Information Technology Act, No. 21, Acts of Parliament, 2000, §§ 67, 67A (India); The Indian Penal Code, No. 45, Acts of Parliament, 1860, § 292 (India).

issue" can divert the discussion away from the victim's autonomy. It will gravitate towards the question of morality, disregarding autonomy and dignity. As exemplified by *Aveek Sarkar v. the State of West Bengal*, the judiciary can be seen gravitating towards a context-driven approach in recent years.[25] However, obscenity legislation is still ill-fitted to deepfake porn. This approach is taken on the ground that the critical harm of deepfake porn is the absence of consent combined with the appropriation of one's identity, beyond just the sexual nature. This consequently doubles down on the harms faced by victims, creating barriers to legal remedies.

4.3 Sexual Offences and Conceptual Incongruities

Those cases in which offenders actually ended up watching or recording the victims, like in the scenario of voyeurism, are ill-suited to deepfake pornography.[26] It is unsuited for the purpose, considering that the deepfake pornographic content is synthetically produced without any real observation or filming of the person. Deepfake pornography produces sexual harm differently. It generates synthetic sexual content through computational methods rather than through physical contact. This is the real doctrinal issue and not that deepfake porn is "less serious." The sexual offence provisions are applied inconsistently from one case to another due to this mismatch.

4.4 Defamation, Impersonation, and the Problem of Partial Fits

Since deepfake pornographic content gravely tarnishes an individual's public standing, people quite often rely on defamation laws.[27] The legal framework regarding defamation disregards the importance of human dignity, personal sexual choices, and psychological well-being, and ends up converting this exploitation into a mere loss of good standing. Conceptualising deepfake abuse narrowly as injury to reputation could diminish how deeply disturbing it feels for those who are impacted by it. It especially happens in settings where patriarchal norms determine how people judge women and sexuality. Take, for example, offences that target improper use of one's identity, such as impersonation and forgery. The legal provisions governing these offences might fit certain scenarios of digital sexual violation, but fall short of operating as the principal groundwork for categorisation. The originally envisaged scope of

[25] Aveek Sarkar v. State of West Bengal, (2014) 4 S.C.C. 257 (India).
[26] The Indian Penal Code*, supra* note 15.
[27] The Indian Penal Code, No. 45, Acts of Parliament, 1860, §§ 499–500 (India).

legal provisions governing these offences was directed towards scams seeking monetary benefits and not towards fictionalised sexual interactions.[28]

4.5 The Pitfalls of Misclassification

In cases where legal ambiguity and vagueness in law prolong victim exposure to institutional processes, the Supreme Court's perturbation on forestalling secondary harm in sexual offense proceedings can be considered more fitting. This is demonstrated in *Nipun Saxena v. Union of India*.[29] When a case is misclassified or categorised incorrectly, it repeatedly leads to foreseeable social and legal outcomes. Those affected are placed at a heightened risk of secondary victimisation. It eventually results in pushing the impacted parties to disengage from the criminal justice system. It is triggered due to protracted procedures, varying charges, and hesitation concerning which legal provisions apply.

Overall, a deficiency in the criminal law of India regarding the legal classification of such acts is exposed by deepfake pornography. Legal responses will continue to be uncoordinated if the law omits to unambiguously recognise this conduct as a form of identity-driven and sexually motivated injury. This interferes with the comprehensive safeguarding of affected individuals and can thus lead to a reduction in legal continuity.

5. Ramifications for Victims

Non-consensual intimate imagery (NCII), notably "deepfake pornography," has proven to be an egregious violation of personal dignity and individual privacy in this rapidly transforming digital ecosystem. There has been a substantial upward trend in deepfake pornography cases in recent times. Cases like the one in Assam emphasised how deepfake pornography sparks social and legal issues. In this case, digitally synthesised explicit images of a past lover were disseminated online.[30] Since there continues to be no standardised method to determine or categorise such content, these events intensify the strain on prevailing legal frameworks.

Deepfake pornography quite often experiences classification errors in present-day legal frameworks. Those impacted may encounter numerous tangible consequences, including but not limited to unsatisfactory legal responses and delayed removal of content. This may

[28] *Id.* §§ 416–419, 463–465.
[29] Nipun Saxena v. Union of India, (2019) 2 S.C.C. 703 (India).
[30] Yunus Dar, *supra* note 20.

contribute to emotional strain and weariness within the institution. Procedural delays have also brought about multiple obstacles. Law enforcement personnel may potentially defer the registration of complaints if they have uncertainty regarding which legal statutes are applicable. At times, they may incorrectly categorise it under erroneous legal categories, or they may forward it to another division entirely. This vagueness hinders the inquiry and may also send signals that the institution is not handling the transgression with due seriousness.

The perpetuation of underreporting trends has become a common norm. A notable segment of victims refrains from filing a formal complaint as they are concerned that they will be met with disbelief or they will be subjected to moral scrutiny regarding the matter.[31] They are apprehensive about their reputation being compromised. Family scrutiny, coupled with setbacks in their professional progress, also inhibits them from reporting the matter. This perpetuates underreporting trends. Hence, those affected are less inclined to report when the law omits to explicitly acknowledge certain harms. This permits culprits to sidestep legal restrictions via loopholes and benefit from such vague stipulations. Institutional barriers are added by social stigma, making it harder to address.[32]

Existing avenues of redress are likely to remain partial and hard for victims to access if the law lacks clear recognition of the "specific harm" caused by deepfake pornographic content. Many victims may see the legal system as "not ready to respond well," and their readiness to stay involved in criminal proceedings over time may decrease. Removal actions and coordination across platforms start later when the harm is not identified early. This reinforces its continued circulation, triggering heightened emotional distress as a result. When these patterns are taken together, they suggest that uncertainty in classification is a gap in doctrine. In addition, it also acts as a tool to further silence victims and wear them down over time.

6. Towards Enhanced Legal Recognition

Just by enhancing clarity on how we interpret the law and how our institutions actually operate within the prevailing criminal law system, we can really make significant improvements. The article argues that introducing new and fresh laws tailored expressly for deepfake pornography is not critical at this stage. By considering deepfake pornography as a form of "sexual identity misappropriation" without consent, it can help us figure out ways to utilise our present-day

[31] Citron, *supra* note 6, at 1906–09.
[32] PRATIKSHA BAXI, PUBLIC SECRETS OF LAW: RAPE TRIALS IN INDIA 89–92 (2014).

legal framework. It thereby precludes the need to force it into a single category that doesn't quite fit.[33]

Given these circumstances, a critical aspect of this work is "the manner in which judges interpret the law". Courts should reinforce the importance of consent, dignity, and harm related to identity. Only then will they be able to see beyond what is considered right or wrong. It will also show how reputations are being affected. All of this can be achieved while still maintaining compliance with legal principles.[34] Law enforcement personnel require unambiguous and precise details for determining appropriate charges. This will afford them greater clarity about what evidence they need to search for. A case in Sonbhadra district, Uttar Pradesh, attracted public attention and exemplified the current functioning of law enforcement in this domain.[35] In this case, nude photographs were synthetically generated using AI tools. These photographs were utilised for extortion of money. This case demonstrated that the preliminary response of the police continues to be highly reactive and involves provisions of cybercrime under the Information Technology Act, 2000. Consequently, tailored capacity-building for the benefit of both police officers and prosecutors is a pressing necessity, along with the adoption of uniform complaint logging protocols. These reforms are a prerequisite for recognising the distinguishing traits of deepfake-facilitated sexual exploitation, most notably its technological and psychological dimensions. Thus, institutional guidance should be regarded as equally important.

In summary, to counteract secondary harm, an interpretive approach centred on victims is the need of the hour. It could help reduce the hesitation of those affected by synthetic sexual content. Ultimately, it could lead to reduced variability in investigative outcomes.[36] This can be achieved solely by leveraging extant legal frameworks more competently. There is, at present, no critical necessity to invent novel laws. By giving prominence to confidentiality, straightforward reporting mechanisms, and collaborative content moderation processes, organisational dedication can be demonstrated to alleviate the pressure on victims.[37] This would foster uniform application of rules and preserve normative equilibrium.

---

[33] Citron & Franks*, supra* note 8.
[34] *Puttaswamy*, 10 S.C.C. at 1.
[35] *AI-Created Obscene Images Used for Extortion, 4 Arrested*, TIMES OF INDIA, (Feb.4, 2026), https://timesofindia.indiatimes.com/city/varanasi/ai-created-obscene-images-used-for-extortion-4-arrested/articleshow/127892891.cms
[36] J.S. VERMA ET AL., REPORT OF THE COMMITTEE ON AMENDMENTS TO CRIMINAL LAW 73–76 (2013).
[37] State of Punjab v. Gurmit Singh, (1996) 2 S.C.C. 384 (India).

7. Conclusion

There is a scholarly consensus that deepfake pornography qualifies as a "critical problem" for criminal law in India, primarily because it is a product of cutting-edge technology. However, this is not the only reason. Another decisive factor is that it fails to fit neatly into prevailing legal categories. Many present-day laws were written with older types of online abuse in mind. However, deepfake pornography has rendered conventional perspectives that are typically accepted difficult to maintain. At the current time, our prevailing legal architecture, such as sections of the Indian Penal Code and the Information Technology Act, 2000, is principally aimed at fragmented aspects of this issue. Their jurisdiction may extend to topics such as obscenity, impersonation, and impairing one's reputation. Nevertheless, they do not adequately address the broader, multidimensional consequences of this phenomenon. These consequences emanate from artificially generated digital content. The most important of these is technology-facilitated sexual harm to an individual's personal identity, which deepfake pornography has the potential to cause.

The main argument of this article is that the core of the issue lies in determining the category of deepfake pornography within our present-day legal architecture. A lacuna or gap in the legal framework may emerge if deepfake pornography is confined to legal categories that are unsuitable. It could also jeopardise the core principles of justice and undermine the efficacy of law enforcement. This could lead to negative outcomes for those who are already affected. Ultimately, this could pave the way for further inappropriate application of this synthetic media technology.

Thus, the article suggests that precise and enhanced legal categories are crucial. Only then can the laws be applied consistently, and those affected can receive real protection. Synthetic technologies are developing at an alarming rate. Hence, criminal law should not be heavily reliant on adding more offences to the statute book. It will remain operational only if critical legal concepts are updated in a precise and consistent manner. This is especially necessary for new modalities of digital sexual abuse.