



ARTICLE

Synthetic Intimacy and Informational Sexual Autonomy: Regulating Deepfake Pornography in India

S K VAISHNAVI*

Abstract

The recent proliferation of deepfakes has disturbed the traditional legal paradigms that regulate image-based sexual harassment in India. Although the existing laws, such as the Information Technology Act of 2000 and the Indian Penal Code, are often used to deal with the distribution of non-consensual intimate images, the underlying conceptual architectures of these laws continue to be rooted in pre-digital notions of obscenity, decency, and defamation. Deepfake pornography is a unique phenomenon, in which the sexual act itself can be completely manufactured, but the harm caused to the reputation, psychology, and dignity of the victims can be very real. This commentary will contend that the current legal architecture in India, which is rooted in obscenity and morality, is normatively and structurally ill-equipped to deal with AI-mediated sexual harms. The article argues that deepfakes reveal a deeper doctrinal gap – the lack of a recognized right to informational sexual autonomy. Unlike other forms of image abuse, deepfakes do not necessarily involve consent to record and distribute intimate information, therefore making it difficult to apply consent norms. Analysis of the recent regulatory measures in India, and also by comparing them to the developments in the UK, United States, and the European Union, this particular commentary argues that to properly regulate deepfakes, we need to move from moral policing to dignity-based regulation.

Keywords- Deepfakes, Sexual Harassment, IT Act, Pornography, Consent

I. INTRODUCTION

In the latter part of 2023 and the early part of 2024, the country of India saw a spate of public outrage over the use of “deepfake” videos generated by AI that targeted women in the public eye. These videos, which were completely fabricated using the increasingly available artificial intelligence software, featured the faces of the women superimposed over the sexually explicit bodies, with a realism that was quite chilling.

Deepfakes are an improvement in the technology of sexual image abuse. Unlike traditional non-consensual sexual image distribution, often referred to as “revenge pornography,” deepfake pornography does not necessarily involve pre-existing sexual images. The issue is not the replication of a private act but the production of a digital image of it. This is a marked departure from the legal standpoint. The Indian criminal law has historically regulated sexualized images through the lens of obscenity, defamation, and the concept of “modesty.” Such a paradigm necessarily requires the presence of obscene material or the violation of a standard of decency.

* Former Assistant Professor, Osmania University.

Deepfakes upset this paradigm: the sexual act has never occurred, and the defamation is immediate and extreme.

According to this commentary, the current legal framework in India, which is mainly governed by the Information Technology Act of 2000 and the Indian Penal Code, is inadequate to deal with the sexual damages inflicted by images created through artificial intelligence. The problem is not merely about the implementation of the law but is, in fact, related to the nature of the law itself. The law regards deepfakes as either obscenity or defamation, which is not the actual damage caused by them. The actual damage is the infringement of the person's right to control their own sexual information. In order to properly deal with synthetic sexual images in the era of artificial intelligence, India should move from moral regulation to a dignity and autonomy-based approach.

II. THE EXISTING LEGAL FRAMEWORK IN INDIA

The current state of law in India to combat deepfake pornography is a mix of various provisions in the law, rather than a comprehensive regulatory framework. The main laws that are applicable in this regard are the Information Technology Act, 2000 (IT Act) and the Indian Penal Code, 1860 (IPC). Although these laws offer some scope for prosecution, a closer look at their conceptual underpinnings shows that they are grossly inadequate in this regard, especially when it comes to AI-created pornography.

a. Information Technology Act, 2000

Section 66E of the IT Act makes it an offense to violate privacy by intentionally capturing, publishing, or transmitting images of a private area without consent. Likewise, Sections 67 and 67A of the IT Act make it an offense to publish or transmit obscene and sexually explicit material in electronic form. At the outset, these sections seem to be amenable to deepfake pornography, particularly when it is posted on the internet.

But these sections themselves assume the existence of an "image" associated with a real private act or body. Deepfakes subvert this assumption. The forged image may not even represent the actual body of the victim; it is a computer-generated construct. Thus, the defense may claim that there was no actual "private area" that was captured or transmitted. The language of these sections, intended to regulate camera-based invasions of privacy, is ill-equipped to deal with AI-generated forgeries that cause the same or greater harm.

Moreover, obscenity-based laws are based on community standards of morality, rather than the rights of the individual whose privacy is violated.

b. Indian Penal Code, 1860

The IPC provides further remedies in Sections 499 (defamation), 354A (sexual harassment), 354C (voyeurism), and 509 (insulting the modesty of a woman). However, these sections expose the structural issues. The law of defamation requires proof of harm to reputation, which must have a minimum visible impact. In the case of deepfakes, the harm is not merely to reputation but also to the psychological, social, and existential parts of a woman. To limit the harm to defamation is to underestimate the gendered and physical components of the issue. Moreover, voyeurism in Section 354C deals with the act of watching or recording a real woman during a private act. Deepfakes, on the other hand, are about creating, not watching. This is a distinction in the law that exposes a loophole. The law criminalizes the secret recording of a real woman. It is less clear about the digital representation of a woman who is completely created.

Most significantly, many of the IPC sections are based on the outdated concept of “safeguarding a woman’s modesty.” The language used in this section is a reflection of the moral paradigm that is based on Victorian values, as opposed to the modern constitutional values of dignity and autonomy. In the case of deepfakes, the problem is not with the loss of modesty but with the theft of identity and the manipulation of sexual agency.

c. The Enforcement and Platform Dimension

Even in instances where the legal provisions are technically applicable, enforcement is not equal. The content is usually hosted on an intermediary and is quickly reproduced on various platforms. Although the rules on intermediary liability create some obligations on due diligence, the “notice-and-takedown” approach is reactive and relies on victims to monitor the internet. This is clearly inadequate for content that can be quickly reproduced.

III. THE CONCEPTUAL PROBLEM: CONSENT, FABRICATION, AND INFORMATIONAL SEXUAL AUTONOMY

Deepfake pornography reveals a fundamental flaw in Indian criminal law, which persists in relying on models of harm that are either caused by the non-consensual distribution of a real sexual act or by the distribution of morally offensive content. Deepfake pornography upends both of these models. There was no sexual act. There may never have been an intimate photograph. But the harm is real, and it is lasting.

a. The Consent Paradox

Consent is the core of modern sexual harm jurisprudence. But deepfakes create what might be called a “consent paradox.” In the traditional non-consensual distribution of intimate images, there is a lack of trust or a lack of consent to distribute a pre-existing image. The legal wrong is stated as unauthorized distribution.

Deepfakes, on the other hand, may lack any pre-existing intimate activity and any pre-existing image to be distributed that requires consent. The wrongdoing is in the creation itself. The law’s preoccupation with whether an actual image was recorded or distributed clouds the issue: does a person have the right to control the sexual depiction of their identity, even if it is only fictional? The Indian legal system lacks a clear articulation of such a right. This creates a problem of doctrine: prosecutors are forced to strain the privacy or obscenity statute to apply to a harm that is, at bottom, identity appropriation and sexual deception.

b. Fabrication and Digital Personhood

Deepfake technology weaponises likeness. By superimposing a person’s face onto explicit content, it constructs a false narrative of sexual conduct that can irreversibly alter public perception. This is not merely reputational damage; it is the technological re-authoring of one’s sexual identity.

The Supreme Court’s landmark decision in Justice K.S. Puttaswamy v. Union of India recognized privacy as intrinsic to dignity, autonomy, and personhood under Article 21 of the Constitution. Yet subsequent statutory interpretation has not fully translated this dignity-based understanding into digital sexual harms. If privacy protects decisional autonomy and personal identity, then deepfakes represent a paradigmatic violation: they fabricate intimate conduct without consent and project it into the public sphere.

Deepfake abuse thus implicates what may be described as “informational sexual autonomy”—the right to control how one’s sexual identity is constructed, represented, and disseminated in informational environments. Unlike modesty-based frameworks, this concept centres agency rather than morality.

c. Gendered Power and Cultural Harm

Deepfake pornography affects women, especially those in public life, more than any other group. This is not different from the general trend of image-based sexual assault, where sexuality is used as a means of social control. In patriarchal societies, damage to reputation through sexualized images may lead to exclusion, professional punishment, and even physical danger.

The Indian criminal law, through its “modesty”-based definitions of crimes, inadvertently perpetuates cultural narratives that associate women’s dignity with sexual purity. However, deepfake pornography shows that the problem is not the loss of modesty but the loss of control over one’s digital self. A dignity-based approach would therefore not rely on purity-based reasoning but instead argue that all people, regardless of gender, have a right to sexual self-definition.

d. Harm without Physical Contact

Another doctrinal discomfort stems from the lack of physical contact. The traditional criminal law favors harm that is physically manifest—bodily harm, physical intrusion, or tangible property loss. Deepfakes are purely information-based. However, psychological pain, reputation damage, and social fallout can be serious and long-lasting.

The inability of current law to comfortably classify such harm stems from an anachronistic ordering system that gives insufficient priority to digital harms. As artificial intelligence technologies continue to erode the distinction between the real and the synthetic, such an ordering system becomes increasingly impractical.

Deepfakes, therefore, indicate not only a gap in regulation but also a conceptual one. Without acknowledging informational sexual autonomy as a protected legal interest, regulatory efforts will continue to be forced into ad hoc amendments to obscenity and privacy laws. The next section will place this problem in the context of comparative regulatory evolution, showing how other countries are beginning, albeit awkwardly, to address synthetic sexual harms.

IV. COMPARATIVE DEVELOPMENTS: EMERGING GLOBAL RESPONSES

Although no country has yet come up with a fully coherent approach to deepfake pornography, a comparison of developments shows that there is a growing trend away from the regulation of obscenity and towards approaches rooted in dignity and safety. The experiences of the United Kingdom, the United States, and the European Union are instructive in this regard.

a. United Kingdom: From Image Disclosure to Synthetic Harm

The UK is now adopting a strategy to address image-based sexual abuse, which is more than just revenge porn. The Online Safety Act 2023 assists online platforms in removing content such as intimate image abuse. New guidelines on sex crimes have now made it an offense to share images without consent, even if you do not intend to harm anyone. The UK’s response demonstrates that they recognize the issue is people not giving consent, not the morality issues. Laws on AI-made images are still being developed but discussions and consultations have begun to recognize AI-

made sexual content as a different issue. The UK government is attempting to prevent image-based abuse. They are creating laws to address the issue.

The Online Safety Act 2023 is one of these laws. It assists in removing content from online platforms. This includes image abuse. New laws on sexual offenses are also being created. They make it an offense to share images without consent. This is true even if you do not intend to harm anyone. The UK's response demonstrates that they care about consent. They recognize it as the issue, not the morality issues. Laws regarding AI-made images are still being discussed. Consultations and conversations have revealed that AI-created sexual content is a large concern. AI-created sexual content is a large concern. The UK is doing its best to prevent image-based abuse. They want to ensure that people feel safe online. The government is creating laws to protect people.

b. United States: Patchwork Criminalization

In the United States, there is still a lack of cohesion in regulation. Some states have passed legislation that specifically targets non-consensual deepfake pornography. For instance, states like California and Texas have made the production or distribution of certain synthetic forms of sexual media, especially in cases of electoral interference and reputation damage, illegal.

At the federal level, there is still a developing framework for addressing AI-generated intimate images, but there is no overarching framework at the national level. The First Amendment free speech issue has a profound impact on the legal discourse in America, making it difficult to criminalize broadly. Consequently, civil causes of action, such as defamation, intentional infliction of emotional distress, or right of publicity, are common avenues for recourse for victims.

The American system is a reflection of both progress and shortcomings, as some states have formally acknowledged synthetic sexual abuse, but the lack of standardized protection means that enforcement is inconsistent.

c. European Union: Risk-Based AI Governance

The European Union is following a trend in that it is creating regulations for artificial intelligence systems. The EU Artificial Intelligence Act examines the risks of AI. Categorizes some applications as high-risk.

It demands information about synthetic content. This Act does not target deepfake pornography specifically. It does demand disclosure of AI-generated content in specific cases.

The EU member states also rely on data protection and dignity rights in the General Data Protection Regulation (GDPR). This regulation is founded on the principle that individuals should have control over their information. This approach emphasizes rights. Is more in line with the principle of individuals having control over their own sexual information. The EU Artificial Intelligence. GDPR complement each other in protecting people's rights. People should have the right to make decisions, about their information and AI-generated content.

d. Lessons for India

Comparatively, three findings are:

1. Consent-Centered Framing Is Crucial – Countries that have moved past the obscenity doctrine and into consent-focused harm definitions provide more rationalized protection.
2. Platform Accountability Matters – Systemic responsibilities of intermediaries are necessary in light of the rapid pace and scope of online distribution.

3. AI-Specific Regulation Enhances Clarity – Directing synthetic media content specifically will help to avoid doctrinal overreach and enforcement ambiguity.

The current state of Indian law is based on outdated criminal laws, which are in contrast to these developing models. Although there are guidelines and removal policies for intermediaries, they are still ad hoc and piecemeal.

V. From Morality to Autonomy: A Normative Framework for Reform

Deepfakes of pornography challenge the Indian legal system with a tough reality: the legal framework for sexualized digital harm is still grounded in morality and not autonomy. A legal provision for obscenity, modesty, or reputation may offer a short-term solution for prosecution, but it does not define the real legal interest. The legal system needs to refocus on dignity and informational control to address AI-generated sexual abuse.

a) Recognizing Informational Sexual Autonomy

The starting point for change would be to accept that people have control over their sexual information. This means that courts or lawmakers would recognize that people have the right to decide what happens to their sexual information. This idea comes from a court case in India, *K.S. Puttaswamy v. Union of India* where it was decided that people have the right to privacy and to make their decisions about their bodies.

Sexual autonomy in the world means that people have the right to control what happens to pictures or videos of them that are sexual in nature. This is important because it means that people can decide who gets to see these pictures or videos and who does not. It does not matter if the pictures or videos are real or not. If someone makes a picture or video of someone without their permission that is wrong. The law could be changed to say that making or sharing sexual pictures or videos of someone without their permission is, against the law even if it is not considered obscene or if it does not hurt the person's reputation. This would help protect people from having their sexual information shared without their consent.

b) Moving Beyond "Modesty" and Obscenity

Second the laws language needs to change. It should use words instead of old-fashioned terms like "modesty" and "morality." These ideas are based on stereotypes, about men and women. They might make people feel bad because of where they come from or who they're

A dignity-based approach would treat everyone fairly. It would focus on the harm caused by taking someone's freedom to make choices. This method would make the criminal law fairer. It would match the ideas of equality and true freedom. It would also stop judges from limiting the harm of deepfakes. They should not just consider community standards or indecency.

The law should protect everyone equally. It should focus on the harm of deepfakes. Deepfakes can cause harm to people. The law needs to address this issue.

c) Calibrated Platform Responsibility

Thirdly, a good reform strategy will have to focus on the environment in which deepfakes spread. An individualized criminal approach is not appropriate in a situation where AI technology is used for anonymous mass-sharing. There must be a clear set of responsibilities for intermediaries to ensure the implementation of fast detection and removal, as well as a grievance redressal system, for synthetic sexual material. But platform responsibility should not lead to over-censorship. There is a need for a balance between freedom of expression and online safety.

d) Integrating Civil and Criminal Remedies

People who are affected by deepfakes want these things to be taken down quickly. They want to be paid back for what happened. They do not want to wait a time for criminal trials to finish. So the law should be changed to include ways for people to get help in court like stopping the deepfake from being shared getting money because of the harm that was done and being able to stay anonymous. This way people can get help from both the criminal sides of the law.

The thing, about deepfakes is that they can hurt everyone and they can also hurt one person badly. We should have courts that just deal with digital problems, like deepfakes so that people can get help quickly. These courts can be called courts or cyber benches. They would be really helpful because deepfakes can spread fast and they can change really quickly.

VI. CONCLUSION

Deepfake pornography is not a new technology it is a big challenge for Indian criminal law. Artificial intelligence can create sexual videos and pictures that are very realistic, and this makes it hard to know what is real and what is not, what is private and what is public, what is a real person and what is just an image. The laws we have now like the Information Technology Act and the Indian Penal Code are a little flexible. They are still based on old ideas about what is obscene and what is modest instead of focusing on people's autonomy.

If the law keeps thinking that fake sexual abuse is a worse kind of indecency, it will not be able to see the real harm it causes, and it will not be able to protect the victims properly. The real harm is that someone's sexual identity is being created without their consent in the world, and this hurts their dignity, which is something that our constitution already says is important.

India has to make a choice about how to deal with this issue. It can keep making changes to the laws and trying to fit new problems into old rules, or it can create a new way of regulating that is based on protecting people's sexual autonomy, making online platforms responsible and protecting people's dignity. In the age of intelligence protecting people's sexual autonomy requires more than just moral rules it requires a big change in how we think about what it means to be a person, in the online world. Deepfake pornography and artificial intelligence are changing things. India needs to think about how to protect people's dignity and autonomy in this new world.