LEX LUMEN RESEARCH JOURNAL- ISSN:3048-8702(O)
Volume 1, Issue 4, Pages:496-509, July 2025

DIGITIZING DESIRE OR FUELING ABUSE? A LEGAL STUDY ON RISE OF AI IN ENABLING SIMULATED SEXUAL VIOLENCE

By- Aishani Aggarwal[1]

ABSTRACT

This research explores the complex and evolving concept of 'digital rape', examining its dual meanings within the Indian legal system and the global context of AI-enabled cyber abuse. While Indian law recognizes non-penile penetration as rape following the 2013 Criminal Law (Amendment) and POCSO Act, global interpretations have expanded to include simulated sexual violence through avatars, deepfakes, and virtual reality—forms of harm that transcend physicality and penetrate psychological and identity dimensions. The study analyzes how Artificial Intelligence, when misused, facilitates acts of sexual violence in digital spaces, with particular focus on deepfake technology. Using qualitative, desk-based methods, the research reveals critical gaps in existing legal frameworks, ethical inconsistencies, and the societal tendency to trivialize virtual sexual assault. It further highlights the psychological trauma suffered by victims, the role of tech companies in mitigating harm, and the inadequacy of both Indian and global laws to address these technologically mediated abuses. The paper advocates for legislative reforms in India, emphasizing consent over intent, and calls for international cooperation to address jurisdictional loopholes in digital sexual violence. The findings contribute to reimagining legal and ethical paradigms suited for an increasingly virtualized world.

KEYWORDS: Digital Rape, Simulate Sexual Violence, Virtual Reality Assault, Deepfakes, AI-enabled cyber abuse, Techno-mediated Violence, Proteus Effect, Cyber Law Reform, Identity-

[1]**Intern, Lex Lumen Research Journal.**

based harassment, psychological trauma in virtual space, Bharatiya Nyaya Sanhita Section 74, Consent vs. Intent, Strict Liability in cybercrimes, Digital Consent, Metaverse Regulation, Avatar-based sexual assault, Virtual legal ethics, Rana Ayyub case, Nina Jane Patel.

INTRODUCTION

In this research paper, we will examine the role Artificial Intelligence (AI) in enabling simulated sexual violence, with a particular focus on the creation and misuse of deepfakes. While AI technology offers advancement in various fields, its potential to do harm has grown significantly, especially in the context of virtual sexual abuse. The lack of legal clarity and adequate protective mechanisms in India has created a series of gaps in safeguarding individuals against such digital violations. Victims of simulated sexual violence often experience psychological and emotional trauma that parallels real-life abuse, yet find themselves without recourse due to the non - physical nature of the harm. This raises a critical question: Should the use of AI in such contexts be viewed solely as a technological failure, or does it reflect a broader social and legal neglect? The objective of this research is to explore how AI, when weaponized through deepfakes technologies, contributes to gender based cyber violence, and whether existing legal frameworks under BNS[2], IT Act[3] and POCSO[4] can or should evolve to address these modern harms.

THESIS ARGUMENT

This paper argues that the unregulated use of AI - generated deepfakes to simulate sexual violence, constitutes a serious form of cyber abuse, and the absence of targeted legal remedies in Indian law

[2] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)

[3] The Information Technology Act, 2000 (No. 21 of 2000)

[4] The Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012)

not only fails to deter such acts but further silences and retraumatizes victims, demanding urgent legislative intervention.

Understanding the dual meanings of 'Digital Rape' in different contexts

The term 'digital rape' holds two distinct meanings in legal and socio-technological contexts, both of which reflect the evolving understanding of sexual violence in the modern era.

1. Global Context - In the International Global discourse, 'digital rape' is increasingly used to describe simulated sexual violence carried out on virtual, augmented, or mixed reality platforms, where the assault occurs through avatars or digital environments, without actual physical contact. This includes the nonconsensual creation and circulation of AI-generated deepfake pornography, immersive virtual reality harassment, or sexual role-playing attacks in metaverse-type spaces. Although there is no physical touch, these acts can cause significant psychological and emotional trauma to the victim, and often blur the lines between real and virtual violation. In most jurisdictions, such as the United States or the European Union, these incidents are emerging challenges under cybercrime, harassment, privacy violation, or image-based sexual abuse laws, under traditional definitions of rape. This redefinition of digital rape signals a shift in the understanding of sexual violence, acknowledging that violation can also be technologically mediated, with serious real-world consequences.
2. Indian Legal Context - In the Indian Legal Framework, however, the tern 'digital rape' refers to the use of fingers (digits), toes, or other body parts excluding the penis to penetrate a women's vagina, urethra, anus, or her mouth without her consent. This has no connection to cybercrime or virtual assault in Indian Law. This meaning was established legally following the Criminal Law (Amendment) Act, 2013, which broadened the definition of rape under Section 375 of the Indian Penal Code (IPC). The instance was first widely recognized when the case of Akbar Ali, Noida Man in Salapur district, committed 'digital rape' on his 3.5-year-old neighbour, lured under the circumstance of providing candy. Until

December 2012, 'digital rape' was considered as molestation and was not considered rape[5]. Previously, only penile-vaginal penetration was recognized as rape. It was after the *Nirbhaya*[6] gang-rape incident that new rape laws were introduced in the parliament and the act was classified as a sexual offence under Section 375 and Protection of Children from Sexual offenses (POCSO) Act. The law was amended to include non-penile penetration (including with fingers or objects) as acts of rape. This change acknowledged the severe violation and trauma inflicted by such acts, which were previously categorised under lesser offences such as "outraging the modesty of a woman". A landmark case that predates the amendment but catalysed reform was *State of Punjab V. Major Singh 1967*[7], in this case, the accused sexually assaulted a seven-month-old baby, but the act was not classified as rape due to the limited definition at the time. He was instead punished for merely outraging modesty, which attracted a minor sentence. This controversial judgement triggered significant debate about the inadequacy of existing laws and later influenced the drafting of more comprehensive protections under both IPC and POSCO which criminalised all forms of penetrative and non-penetrative assault against children.

Thus, 'Digital Rape' is a term with dual meanings, shaped by jurisdiction, technology and evolving socio-legal awareness with varying definitions in different countries.

Role of Tech Companies in mitigating 'Digital Rape'

[5] Abhishek Awasthi, Know what is 'digital rape' for which Noida man gets life in prison, Firstpost.(August 31, 2022, 18:15:19 IST), https://www.firstpost.com/india/know-what-is-digital-rape-for-which-noida-man-gets-life-in-prison-11155141.html

[6] Mukesh & Anr vs State For Nct Of Delhi & Ors, AIR. 2017 SC 2161

[7] State of Punjab V. Major Singh, AIR. 1967 SC 63 (India)

The role of Tech companies in mitigating 'digital rape', platforms like social media, gaming environments, and VR systems are frequent settings for such violations[8]. Especially in the realm of Virtual Reality (VR), Augmented Reality (AR) and AI-based platforms, it is central to preventing abuse, enforcing digital safety and ensuring ethical Tech development. Platform Design and Safety Features - Tech companies such as Meta. formerly Facebook, Roblox and other developing metaverse platforms bear responsibility for building safety by design, embedding features that protect users in virtual environments. Creating default safety boundaries like personal bubbles or interaction limits especially for avatars that simulate human presence using AI moderation tools to detect and respond to abuse reports in real time like gestures, verbal harassment and unwanted proximity.

Meta introduced a "Personal Boundary" feature in 2022, which prevents avatars from coming closer than 4 feet to another user's avatar. It is intended to create a feeling of physical space and avoid unwanted interactions as a default setting in "Horizon Worlds" and other meta VR experiences, the tool however has drawbacks as it failed to become active right after logging in. This tool was introduced after cases of harassment including that of *Nina Jain Patel,* that gained media attention. Nina Jain Patel, an Indian origin psychotherapist and educational tech startup founder living in the UK, within 60 seconds of logging into the Metaverse, her avatar was verbally and sexually harassed by a group of men's avatars. They verbally taunted her, demanded compliance and her avatar was virtually gang-raped. Although the incident occur in a digital in environment the emotional distress suffered by Nina was real and intense she described the experience as "surreal and horrible" with lasting psychological trauma akin to real sexual assault. Nina was said to experience the Proteus effect[9], which is the tendency for people to be affected by

[8] Aadya Khanna, Understanding Virtual/Digital Rape: Navigating Consent and Accountability in the Digital Age, The Centre for Law and Policy Research, Jan 30, 2025, https://clpr.org.in/blog/understanding-virtual-digital-rape-navigating-consent-and-accountability-in-the-digital-age/#:~:text=Virtual%20or%20digital%20rape%20includes,sexual%20advances%20or%20simulated%20assaults.

[9] Martin Coesel, Anna et al. "A theoretical review of the Proteus effect: understanding the underlying processes." Frontiers in psychology vol. 15 1379599. 26 Jun. 2024, doi:10.3389/fpsyg.2024.1379599

their digital representations, such as avatars, dating site profiles and social networking personas. Typically, people's behaviour shifts in accordance with their digital representatives.[10] This incident gained global recognition, which also led to the rise in heated debates of whether 'Digital Rape is Real Rape?' and is it comparable to the physical trauma experienced by Victims, outside the virtual realm.

Trivialization of Virtual Sexual Violence and its Implications

The trivialization of sexual violence within the metaverse, often referred to as 'virtual rape' or 'meta-rape', stems from the stigma of comparing assault involving physicial contact and the assault virtually experienced by the victims. It has significant implications for how these experiences are perceived in the real world, as this dismissal is rooted from the perception of the metaverse as a separate, less real realm, leading to a distinction between real and virtual crimes. The idea that these acts are merely simulations or play can foster a sense of entitlement to engage in harmful behavior, leading up to desensitization to the real world, without accountability. This perspective can downplay the seriousness of the harms experienced, drawing parallels to how online abuse is sometimes minimized compared to offline abuse.

The tendency to trivialize meta-rape risks perpetuating a dualistic understanding that segregates online and offline spheres and virtual from real-world experiences. This approach overlooks the interconnected continuum of gendered and sexualized harms and fails to acknowledge the seamless transition between technology-facilitated and offline experiences of sexual violence, where the comparison undermines the trauma experienced by victims. Victims often report psychological trauma from virtual experiences that is comparable to real-life trauma. For Example, since 2018, Rana Ayyub has been subjected to brutal online harassment, including - Deepfake Pornography & Morphed Videos, her face was superimposed onto pornographic videos using

[10] Nina Jane Patel, Sexual Harassment in VR, The Proteus Effect and the phenomenology of Darth Vader — and other stories.., Medium, Dec 21, 2021, https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0

deepfake technology, falsely portraying her in sexual acts. These were widely circulated on WhatsApp, Twitter, and Facebook, with the aim to defame and silence her[11]. This instance highlights the gaps in the cyber laws for protection against deepfakes that can alter one's reputation irrevocably, with no recourse left.

When these metaverse experiences are dismissed, it mirrors societal tendencies to downplay harms like image-based sexual abuse, where the fake nature of altered imagery is used to undermine victims' valid experiences, or even cause damage and harm to reputation and character of the victim. The minimization of these harms also affects criminal investigations, as current laws may be perceived as inapplicable, and prosecutors might accept a defendant's claim of not considering the conduct harassment. This creates a situation where victims have no recourse until society recognizes the harm as criminal, thus often being dismissed and not taken seriously.

Current Global laws and their inadequacy to address virtual violations

Current laws may inadequately address image-based sexual abuse due to several shortcomings, generally rooted in bias against the unexplored complexities of this form of cybercrime. The US Malicious Deep Fake Prohibition Act[12], for instance, has been criticized for its overbroad definition of deepfakes, which could unintentionally encompass legitimate content like computer-generated imagery in films or be used for parody and satire without addressing the harm caused to individuals whose likeness is used without consent. In contrast, the UK Revenge Pornography Guideline[13] requires an intention to cause harm for charges to hold, potentially allowing for significant leeway for abuse even when consent for data processing is absent. This underscores a

[11] Halt all retaliation attacks against Indian journalist Rana Ayyub – UN experts, UN News, 21 February 2022, https://news.un.org/en/story/2022/02/1112362

[12] US Malicious Deep Fake Prohibition Act of 2018, 18 U.S.C., (115th Congress 2018), Bill

[13] Section 33 of the Criminal Justice and Courts Act 2015

need for legislation to prioritize explicit consent for dissemination as a primary defense, irrespective of other intent. Furthermore, the effectiveness of any law hinges on its enforcement; without robust implementation, enacted laws may not serve as a sufficient deterrent or fulfill government promises regarding human rights and safety, thus further rendering no actual recourse to the victims. The global nature of digital technology also presents challenges, as applying the law of one jurisdiction becomes difficult when perpetrators reside in another, particularly if the abuse is not prohibited in their jurisdiction of residence, which often turns into an international dispute between individuals of two countries, generally resulting in the perpetrator walking free. For example, in April 2007, Brussels police began an investigation of the alleged virtual rape of a Second Life user as reported by two Belgian newspapers, which led to and across border investigation but did not bring to fruitation, carrying out of justice for the victim, because there are no real legal repercussions for virtual rape, there are also very few officially noted cases of these offenses[14]. This was one of the few cases that failed to prosecute the perpetrator, due to inadequacy of laws.

The rapid advancement of deepfake technology outpaces legal reforms, creating a gap where the law struggles to keep pace with the harms being perpetrated. This is exacerbated by the increasing ease with which deepfakes can be created using readily available mobile applications and Artificial Intelligence technology leading to a potential chaotic circumvention of consent through deepfake pornography. For example, the US Congress introduced bills like the Malicious Deep Fake Prohibition Act of 2018 and the DEEPFAKES Accountability Act[15], but criticisms have been raised about their broad definitions that may not sufficiently target malicious intent or protect victims adequately. The challenge in attribution, where identifying the perpetrator of pornographic deepfakes is difficult due to anonymizing technology and insufficient metadata, leading to perpetrators to evade real consequences for their actions, which further hinders the application of

[14] Melissa Mary Fenech Sander, Questions about accountability and illegality of virtual rape, Pg. 7, 2009

[15] DEEPFAKES Accountability Act, H.R. 5586, 118th Cong. § 1041

law. Consequently, victims may bear the high cost of civil suits, necessitating intervention from non-governmental organizations.

Immoral utilization of deepfakes to fuel Rape Fantasies

There is a need to address potential contradictions regarding the morality of fictional depictions of immorality by distinguishing between two types of enjoyment: enjoyment qua simulation and enjoyment qua substitution. Enjoyment(sim) is the enjoyment of the fictional representation itself, regardless of whether it depicts an immoral act. In contrast, enjoyment(sub) involves desiring what the simulation represents, rather than the simulation itself, essentially using the simulation as a substitute for a real, but unattainable, desire[16]. Gratification of rape fantasy using robots, through enjoyment(sub) is considered immoral because it reflects a desire for the actual act to occur. This is because the enjoyment is derived from fulfilling a vicarious desire for the real, even if that desire is motivationally inert as explained by the author Garry Young. In such cases, the enjoyment is problematic because it signals a desire to enact the immoral act in reality, regardless of whether that desire is acted upon. This distinction is crucial because it separates enjoying the simulation of a taboo as a simulation from desiring the actual taboo act.

METHODS

This Research was based on a qualitative, desk-based approach. The data was primarily collected from publicly available online sources including search engines such as Google and Video content platforms (primarily) YouTube. A variety of secondary materials such as news articles, expert interviews, research summaries, educational content and commentaries were reviewed to gather insights relevant to the topic. The selection of resources was guided by relevance, credibility and

[16] Volume 42, Garry Young, Journal of Applied Philosophy, Pg. 2, Feb, 2025

recency. Preference was given to content created or endorsed by professionals, educators and subject matter experts. Videos from verified or reputable channels were prioritized to ensure reliability. Educational content from professionals was reviewed to understand the core perspectives. No primary data collection such as interviews, surveys, or experiments was conducted as the study focused on synthesizing existing knowledge and opinions from digital media and online literature.

RESULTS

Digital rape represents a dual spectrum violation that simultaneously reflects the bodily invasion in the physical realm (as in the Indian legal context) and the physiological, identity-based violation in virtual spaces (global/cyber context). Both forms challenge traditional legal definitions of sexual violence and require a reimagined legal-ethical framework that transcends physicality and considered psychological impact, identity misuse, and techno-meditated assault.

Dimension	**Indian Law**	**Global Law**
Definition	Non-penile penetration (E.g. with toes or fingers)	Simulated sexual assault via avatars, AI, Deepfakes, VR abuse
Legal Recognition	Post 2013 IPC Amendment and POCSO	Ambiguous under cybercrime, privacy, or harassment laws
Nature of Violation	Bodily autonomy, physical trauma	Identity invasion, emotional trauma, psychological manipulation

Societal Response	Stronger post Nirbhaya Reforms	Often trivialized and not seen as 'real'
Ethical Complexity	Less Debated and is morally unambiguous	Questions around fantasy vs intent are given priority and how substitution of simulation can be deemed immoral.

LEGAL REMEDIES

Legal Remedies that can be adapted by the legislators to provide recourse to the victims:

1. Specific Legislation - Specific statutory legislation for cybercrimes and offences dealing with meta-verse, virtual reality, augmented reality and mixed reality. This will ensure offence specific punishments and ingredients to classify the offences into cognizable and non-cognizable offences.
2. Outrage of Modesty - Section 74, Bharatiya Nyaya Sanhita to be inclusive of cyberspaces and virtual reality spaces where the avatars might or might not be exposed to explicit nudity or sexual images whether real or unreal. Image based AI, is a popular form of AI, that if fallen in the wrong hands, can be misused and be taken advantage of while users hide behind the mask of anonymity.
3. Broaden definition in existing cyberlaws - Explicitly include the definitions to use words like deepfakes, avatar-based experience and simulated immersiveness as real form of experience and consider the 'Proteus Effect' and its application.
4. Shift the focus - Put emphasis more on 'Lack of Consent' more than 'Intent to Harm', focusing on Actus Reus as compared to Mens Rea. This allows the application of strict liability concept, rather than putting emphasis in determining the guilty mind of the perpetrator to evade liability.

DISCUSSION

The research finding reveal a fundamental challenge in how legal systems both in India and globally, respond to the evolving nature of sexual violence in the digital era. The dual interpretation of 'digital rape' encompassing both physical non-penile penetration and simulated sexual assault via avatars, AI, or deepfakes demand a broader and more nuanced legal lens that considered bodily, emotional, and identity-based harm.

1. Reconceptualizing Sexual Violence Beyond Physicality- Traditional legal frameworks are heavily grounded in the tangibility of assault, emphasizing physical force, contact, or penetration. However, the global understanding of digital rape shifts the focus from bodily autonomy to identity autonomy, where the violation is psychological, reputational, and symbolic in nature. This transformation of violence into techno-mediated harm echoes what scholars like Danielle Citron and Mary Anne Franks have previously argued, that digital abuse can be as destructive as physical abuse due to its omnipresence, permanence, and amplification via digital platforms.[17] The Indian legal context, particularly after the 2013 Criminal Law (Amendment) Act and the POCSO Act, clearly defines and punishes non-penile sexual penetration. However, in global contexts, no unified statute exists to address simulated or virtual assaults, leading to inconsistent protections, as seen in cases like Nina Jane Patel's experience in the metaverse.
2. Implications for Legal Reform and Ethics- One of the key findings is the 'ethical dissonance' in addressing simulated sexual violence. While Indian Laws treat physical digital rape as morally and legally indefensible, the global discourse is fragmented, often caught in a debate between fantasy rights and victim impact. This raises questions about moral thresholds, especially in contexts where avatars are misused in immersive VR experiences or where AI-generated deepfakes simulate real individuals in sexually explicit

[17] Citron, Danielle Keats. Hate Crimes in Cyberspace. Harvard University Press, 2014. JSTOR, http://www.jstor.org/stable/j.ctt7zsws7. Accessed 21 July 2025.

ways. The builds upon previous studies like Henry & Powell, 2016[18] which argue that the lack of legal frameworks for such virtual violations contributes to a trivialization of trauma, causing secondary victimization and reduced reporting. This research confirms that victims in such digital cases experience emotional trauma, fear, and reputation damage, a psychological toll comparable to real-world sexual abuse.

3. Comparative Legal Challenges- The data also illustrates the legal asymmetry between jurisdictions. The difference in interpretation of the term 'digital rape', underscores the urgent need for global legal harmonization. The absence of any international treaty or convention on virtual sexual crimes enables perpetrators, especially in cross-border situations, to exploit jurisdictional gaps and escape accountability. It is suggested the creation of standardized global protocols, similar to the 'Budapest Convention on Cybercrime'[19], to tackle virtual sexual offenses with cross-border implications.

CONCLUSION

The findings of this research underscore the urgent need to reconceptualize the legal and moral boundaries of sexual violence in an age where technology has outpaced regulation. 'Digital rape' is no longer confined to the physical domain; it now includes virtual and simulated acts that produce real psychological, emotional, and reputational damage. The Indian legal system has taken progressive steps in expanding the definition of rape to include non-penile forms of penetration, yet remains unequipped to handle virtual sexual violations enabled by AI, avatars, and deepfakes. Globally, the absence of a standardized legal framework and the lack of clarity in jurisdictional responsibility create loopholes that are often exploited by perpetrators, further compounding

[18] Powell, Anastasia, and Nicola Henry. "Technology-Facilitated Sexual Violence Victimization: Results From an Online Survey of Australian Adults." Journal of interpersonal violence vol. 34,17 (2019): 3637-3665. doi:10.1177/0886260516672055

[19] Convention on Cybercrime, ETS No. 185, or European Treaty Series No. 185

victim trauma. The trivialization of virtual sexual assault reflects a societal failure to recognize the continuum of harm between the digital and physical realms. Victims such as Nina Jane Patel and Rana Ayyub demonstrate how deeply personal and damaging these cyber violations can be, even when no physical contact occurs.

This paper calls for an urgent overhaul of cyber and sexual violence laws in India and internationally. Legal reforms must emphasize lack of consent over intent, adopt strict liability principles, and acknowledge the 'Proteus Effect' and identity-based harms as legitimate grounds for legal recourse. Tech companies must also be held accountable through policy and platform design that prioritizes user safety by default. In a world increasingly shaped by immersive and AI-driven interactions, the failure to recognize and legislate against techno-mediated sexual violence not only silences victims but risks normalizing a new frontier of abuse. Lawmakers, ethicists, and technology developers must work in tandem to close this gap before the virtual becomes indistinguishable from the real world, not only in experience, but in law and justice.