



# INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

**IJLAR**

+91 70421 48991  
editor@ijlar.com  
www.ijlar.com

## **DISCLAIMER**

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

## **Introduction**

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

## **Preface**

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

## **Description**

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

# **DIGITAL SEXUAL VIOLENCE THROUGH ARTIFICIAL INTELLIGENCE: A STUDY OF TRAUMA, STIGMA AND VICTIM – ORIENTED LEGAL REFORM**

AUTHORED BY - ARJA BHANU PRIYA

## **Abstract**

The rapid evolution of artificial intelligence has generated a new class of sexual offences, including deepfake pornography, nudification, AI-generated child sexual abuse material (CSAM), and synthetic sexualised imagery. These offences do not require physical contact; yet they inflict profoundly destructive psychological, emotional, and social harm. Victims - primarily women, minors, journalists, and individuals with a public digital presence - experience identity violation, reputational damage, sexual humiliation, and long-term trauma. India's legal framework remains fragmented across the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita (BNS), 2023, POCSO, and the IT Rules, 2021, none of which adequately conceptualise or criminalise AI-synthetic sexual violence. This paper integrates doctrinal analysis, trauma psychology, feminist jurisprudence, and global regulatory models to present a comprehensive, victim-centric legal framework for India. Grounded in constitutional morality—particularly Articles 14, 19, and 21 the article argues for a unified statute that recognises AI-based sexual offences, mandates platform accountability, ensures fast-track takedowns, guarantees confidentiality, and provides psychological rehabilitation and compensation. It concludes that failing to address AI sexual harms violates India's constitutional obligations, international commitments under CEDAW, and fundamental principles of digital dignity and gender justice.

**Keywords:** Deepfake pornography, AI sexual offences, psychological trauma, social stigma, digital dignity, constitutional morality, gender justice, synthetic CSAM.

## 1. Introduction

Deepfake pornography constitutes 90–96% of all deepfake content worldwide, targeting primarily women and minors.<sup>1</sup> Victims include celebrities, journalists, students, and ordinary women, whose digital identities are misused due to abundant online images.<sup>2</sup> Deepfakes constitute a form of *digital sexual assault*, inflicting psychological trauma and reputational destruction equivalent to real sexual harm.<sup>3</sup>

In India, these harms are magnified by patriarchy, moral policing, and institutional apathy.<sup>4</sup> Despite *Puttaswamy* recognising privacy, dignity, and bodily integrity as fundamental rights,<sup>5</sup> current statutory frameworks remain technologically outdated.

## 2. Conceptual Foundations of AI-Based Sexual Offences

Deepfakes are generated using GANs (Generative Adversarial Networks) and diffusion models that synthesise hyper-realistic images.<sup>6</sup> Face-Swap Pornography, Victim's face is superimposed onto sexually explicit bodies. Creates "realistic" sexual imagery without consent. Nudification Tools, AI removes clothing digitally from images. Synthetic CSAM, AI creates sexualised minors who may not exist.<sup>7</sup> AI Erotic Chat, Fake sexual conversations fabricated using AI language models. Voice-Based Abuse, AI clones voices using small audio samples. Full-Body Avatars, AI generates entire synthetic sexualised avatars resembling the victim.

- 
1. Furizal et al., *Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography*, 12 **Soc. Sci. & Human. Open** 101882 (2025).
  2. Siddharth Johar, *Articulating a Regulatory Approach to Deepfake Pornography in India* (2023).
  3. Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 **Cal. L. Rev.** 1753 (2019).
  4. Saloni S. Patil & S.P. Mishra, *Legal Gaps in Addressing Revenge Porn and Deepfake Pornography in India*, 7 **IJMRSET** 14935 (2024).
  5. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
  6. Ian Goodfellow et al., *Generative Adversarial Networks*, 63 **Communications of the ACM** 139 (2020).
  7. Pallvi & Vinit K. Sharma, *Regulating Deepfake Technology in CSAM*, 6 **IJRPR** 3429 (2025).
  8. Citron & Chesney, *supra* note 3.
  9. Claire McGlynn et al., *Image-Based Sexual Abuse*, 21 **Feminist Legal Stud.** 25 (2017).
  10. Patil & Mishra, *supra* note 4.
  11. Johar, *supra* note 2.
  12. Narmadha L., *AI-Generated Deepfake Sexual Offences in India*, 5 **IJARST** 259 (2025).

### 3. Psychological Trauma in AI-Based Sexual Offences

Identity Violation, Victims equate deepfake harm to “digital rape.”<sup>8</sup> Loss of Control, Content circulates endlessly, causing helplessness. Hyper vigilance, Victims repeatedly check the internet for resurfaced content. Perpetual Victimization, Every re-upload retraumatizes the victim.<sup>9</sup> Self-Esteem Damage, Victims develop shame, guilt, and body dysmorphia. Social Withdrawal Trauma leads to isolation and depression.

### 4. Social Stigma in India

Patriarchal Norms, Society blames women even for fabricated images.<sup>10</sup> Family Honour, Victims face pressure to remain silent.<sup>11</sup> Professional Consequences, Stigma affects employment, academics, and relationships. Underreporting, Victims avoid filing complaints due to shame, fear, and police insensitivity.<sup>12</sup>

### 5. Legal Framework in India: Doctrinal Gaps

#### 5.1 Information Technology Act, 2000 – An Outdated Legal Architecture

The IT Act was drafted in an era when AI-generated synthetic media did not exist. Sections 66E, 67, and 67A criminalise the *capture, transmission, and publication* of obscene or sexually explicit material.<sup>13</sup> However, these provisions presuppose, a real act, a real body, and a real sexual event.

Deepfakes do not involve actual nudity or sexual activity. Instead, they involve *synthetic sexualisation of identity*, which the statute does not recognise. As Patil & Mishra note, Indian law “struggles with gaps in specificity” for synthetic pornography.

#### Why IT Act fails for deepfakes:

1. “Obscenity” is defined around real content, not AI-generated imagery.
2. Consent standards in the IT Act apply only to photographs/videos actually taken.
3. No recognition of synthetic CSAM, unlike the EU AI Act (placing deepfakes under high-risk AI).

---

13. Information Technology Act, 2000, S 66E, 67, 67A.

14. Narmadha L., supra note 12.

4. Police often dismiss complaints since “video is fake”

Thus, the IT Act is technologically outdated and doctrinally inadequate.

## 5.2 Bharatiya Nyaya Sanhita (BNS) 2023 — Structural and Conceptual Limitations

BNS replaces IPC but does not modernise sexual offence definitions to include AI-generated harm. Subsequent provisions on voyeurism, modesty, obscenity, identity fraud all assume real-world physicality. Deepfake pornography involves no real capturing device, no real sexual act, no real nudity, no physical intrusion. Hence, BNS cannot categorise deepfake crimes under existing definitions. Narmadha L. highlights this gap: AI sexual offences “fall outside traditional sexual offence categories.”<sup>14</sup>

### Key Problems:

- Outraging modesty requires physical presence.
- Voyeurism requires real, private acts.
- Obscenity requires real sexual content.
- Identity theft is not treated as sexual harm.

BNS therefore fails to recognise that identity sexualisation is itself sexual violence.

## 5.3 POCSO Act, 2012 – Limitations with Synthetic Minor Imagery

POCSO criminalises sexually explicit depictions of children. But deepfakes create two doctrinal conflicts:

### (a) What if AI creates a completely fictional child?

POCSO requires a “*child*,” meaning a real human under 18. Synthetic children are not legally “children” yet the harm (pedophilic gratification, grooming material) is real. Pallvi & Sharma confirm: Indian law does not mention synthetic CSAM.<sup>15</sup>

### (b) What if an adult image is age-regressed using AI?

Is the adult victim protected?

Is the product considered CSAM?

---

15. Pallvi & Sharma, supra note 7.

### (c) What about face-swapped CSAM?

If a minor's face is placed on an adult body, does it constitute abuse? Current law gives no clear answer.

Because of these doctrinal ambiguities, many cases collapse during investigation and trial.

## 5.4 Weak Intermediary Liability and Platform Accountability

Under Section 79 IT Act and IT Rules (2021), intermediaries are required to remove unlawful sexual content, but deepfakes are not explicitly listed, Platforms hesitate to remove content without court orders, "Obscenity" definitions are unclear, lack of mandatory AI-detection tools. Shinu Vig observes that platforms avoid responsibility due to "absence of deepfake-specific liabilities."<sup>16</sup> This weakens victim support and allows synthetic pornography to circulate freely.

## 5.5 Evidentiary Crisis under the Bharatiya Sakshya Adhinyam (2023)

Deepfakes destabilise core foundations of evidence law—authenticity, integrity, reliability. Singh & Panta warn "Deepfake evidence threatens the presumption of innocence and the right to a fair trial."<sup>17</sup> Key evidentiary dangers are fake confessions created via voice deepfakes, fake CCTV evidence synthetically altered, fabricated chats and screenshots indistinguishable from real ones, judges and police lack AI forensic training.

Thus, procedural justice collapses if courts cannot determine whether evidence is genuine.

## 5.6 Deepfake Prevention & Criminalisation Bill (2023) — A Missed Opportunity (Still Pending)

The Bill proposes deepfake definitions, watermarking requirements, criminal penalties, a National Deepfake Task Force.<sup>18</sup> However, it remains unenacted, meaning India still lacks a direct statutory response. Until passed, victims continue facing criminal, procedural, and technological barriers.

---

16. Shinu Vig, *Regulating Deepfakes: An Indian Perspective*, 17 **J. Strategic Security** 70 (2024).

17. Harmanjeet Singh & Ritu Panta, *Deepfake Evidence & Indian Criminal Justice System*, 7 **IJFMR** (2025).

18. *Deepfake Prevention and Criminalisation Bill*, No. LXX of 2023.

## 6. Comparative International Approaches

### 6.1 United States

US states like Virginia, Texas, and California have enacted deepfake laws criminalising non-consensual AI pornography. The TAKE IT DOWN Act provides minors with rapid takedown remedies.

#### Strengths:

- fast takedowns
- civil + criminal remedies
- focus on minors

#### Weaknesses:

- No uniform federal law.
- State-wise fragmentation leads to inconsistent protection.

### 6.2 United Kingdom

The Online Safety Act 2023 recognises deepfake porn as sexual harm, mandates platform assessments, imposes multimillion-pound penalties through OFCOM.

UK model is highly regulatory and state interventionist - useful for India's context.

### 6.3 European Union

The EU Artificial Intelligence Act (2024) classifies deepfakes as high-risk AI, mandating watermarking, metadata disclosure, transparency and consent for biometric manipulation.<sup>19</sup>

Combined with GDPR's Right to Be Forgotten, EU offers the strongest victim protections globally.

### 6.4 Australia

Under the Online Safety Act 2021, Australia empowers its eSafety Commissioner to issue 24-hour takedown notices, penalise platforms, address both minors and adults.

Australia's harm-based approach offers rapid relief.

---

19. European Union, *AI Act* (2024).

## 6.5 Lessons for India

India needs:

- A unified national statute,
- Strict platform obligations,
- Recognising deepfake harm as sexual violence,
- Rapid takedowns similar to Australia,
- Clear definitions like EU AI Act.

## 7. Constitutional Morality & Digital Dignity

### 7.1 Article 21 — Privacy, Dignity, Bodily Integrity<sup>20</sup>

In *Puttaswamy*, SC held privacy includes sexual privacy, decisional autonomy, informational control, bodily integrity. Deepfake pornography destroys all four. Victims lose control over their identity, sexual dignity, and bodily representation.

### 7.2 Article 14 — Equality Before Law

Women disproportionately suffer deepfake sexual violence. Failure to protect women from synthetic abuse constitutes indirect discrimination, gender-based violence, state failure to ensure equality.

### 7.3 Article 19 — Reputation & Expressive Autonomy

In *Subramanian Swamy*, SC held reputation is part of Article 21 rights.<sup>21</sup> Deepfakes destroy reputation, hinder employment, affect marriage prospects and violate expressive autonomy

### 7.4 International Commitments (CEDAW)

Under CEDAW, India must protect women from all forms of gender-based violence; including cyber-violence.<sup>22</sup> Non-action violates international obligations.

---

20. *Puttaswamy*, supra note 5.

21. *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221.

22. CEDAW, 1979.

## **8. Victim-Centric Legal Framework for India (Expanded)**

### **8.1 Statutory Definitions**

The law must define deepfake pornography, synthetic CSAM, nudification, voice cloning, identity sexualisation. Clarity prevents legal ambiguity and strengthens enforcement.

### **8.2 New Offence in BNS**

India must introduce a separate chapter in BNS criminalising creation/dissemination of AI-sexual content, strict liability for creators/distributors, aggravated punishment when minors are involved. This aligns with UK and EU models.

### **8.3 Presumption of Non-Consent**

Deepfakes are *never consensual*. Burden should fall on creators, disseminators, platforms. Victims need not prove non-consent.

### **8.4 Mandatory 24-Hour Takedown**

Platforms must remove deepfake sexual content within 24 hours, like Australia's law. This prevents spread, re-traumatisation, and viralisation.

### **8.5 One-Stop Digital Sexual Violence Centers**

Centers providing mental health counseling, legal assistance, cyber-forensic support, immediate take down help. Victims must not navigate the system alone.

### **8.6 Confidentiality Protections**

Courts must ensure sealed records, suppressed victim identity, in-camera trials. This reduces stigma and encourages reporting.

### **8.7 Digital Dignity Compensation Scheme**

Victims suffer therapy costs, reputational loss, education/workplace discrimination. Government must fund compensation via a dedicated scheme.

### **8.8 Platform Accountability**

Platforms must deploy watermarking, use hash-matching databases, preserve metadata for investigation, identify origin of deepfakes, employ AI forensic tools. This shifts responsibility away from victims.

### **8.9 Forensic Infrastructure**

India needs a National Deepfake Forensics Laboratory, similar to EU's AI verification system. This lab must master GAN fingerprinting, diffusion model detection, reverse engineering, metadata verification.<sup>23</sup> Without forensic capabilities, justice collapses.

### **8.10 Right to Be Forgotten**

Victims must have legal power to demand digital erasure, removal from search engines, deletion from platforms. Courts should grant urgent ex-parte orders in deepfake case.

## **9. Conclusion**

AI-based sexual offences represent a technologically advanced form of gender-based violence. India must adopt a unified statute that criminalises AI sexual harm, mandates platform accountability, guarantees victim-centric remedies, and upholds constitutional morality.

---

23. Singh & Panta, supra note 17.