INTERNATIONAL JOURNAL OF

MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

Legal Gaps in Addressing Revenge Porn and Deepfake Pornography in India: A Socio-Legal Analysis

Saloni Shashank Patil, Dr. S.P. Mishra

Ph. D Research Scholar, Department of Law, Chhatrapati Shivaji, Maharaj University, Panvel, Navi Mumbai, India

Professor and HOD, Department of Law, Chhatrapati Shivaji Maharaj University, Panvel, Navi Mumbai, India

ABSTRACT: The rapid proliferation of digital technologies in India has given rise to new forms of cybercrimes, notably revenge porn and deepfake pornography, which pose significant threats to privacy, dignity, and gender equality. Despite the existence of the Information Technology (IT) Act, 2000, and provisions under the Indian Penal Code (IPC), 1860, India's legal framework struggles to effectively address these emerging challenges due to gaps in specificity, enforcement, and socio-cultural alignment. This research paper conducts a socio-legal analysis of the legal gaps in tackling revenge porn and deepfake pornography, examining the IT Act, IPC Sections 354C and 509, and judicial interpretations like State of West Bengal v. Animesh Boxi (2018). It explores socio-cultural factors, such as patriarchal norms and victim-blaming, that exacerbate these issues, and assesses enforcement challenges in the digital age. Drawing on comparative insights from international frameworks, such as the UK's Sexual Offences Act, 2003, the paper proposes legislative reforms, enhanced enforcement mechanisms, and public awareness strategies to strengthen India's response, aligning with constitutional guarantees under Articles 14, 21, and international standards like CEDAW.

KEYWORDS: Revenge Porn, Deepfake Pornography, Cybercrime, Information Technology Act, Indian Penal Code, Socio-Legal Analysis, Gender Equality, Privacy, Legal Reforms, Digital Age.

I. INTRODUCTION

The advent of digital technologies in India has ushered in new forms of cybercrimes, notably revenge porn and deepfake pornography, which pose severe threats to individual privacy, dignity, and gender equality. These practices, often rooted in patriarchal norms and amplified by social media, exploit victims—predominantly women—through non-consensual dissemination of intimate imagery, challenging constitutional guarantees under Articles 14 (equality) and 21 (privacy, dignity). The legal framework, primarily the Information Technology (IT) Act, 2000, and sections of the Indian Penal Code (IPC), 1860, such as 354C and 509, seeks to address these issues but struggles with gaps in specificity and enforcement. Socio-legal analyses highlight how socio-cultural factors, including victim-blaming and gender stigma, exacerbate these challenges, deterring victims from seeking justice. This research paper conducts a socio-legal analysis of the legal gaps in tackling revenge porn and deepfake pornography, examining the IT Act, IPC provisions, and judicial decisions like Avnish Bajaj v. State (2005). It explores enforcement challenges, socio-cultural influences, and proposes legislative reforms, enhanced enforcement, and public awareness strategies to align with constitutional mandates and international standards like CEDAW. The objectives are to assess legal deficiencies, analyze socio-cultural barriers, and recommend measures to strengthen India's response to these digital-age challenges, ensuring protection for victims and gender equity.

II. LEGAL FRAMEWORK ADDRESSING REVENGE PORN AND DEEPFAKE PORNOGRAPHY

India's legal framework for addressing revenge porn and deepfake pornography primarily comprises the Information Technology (IT) Act, 2000, and relevant sections of the Indian Penal Code (IPC), 1860, operating within the constitutional guarantees of equality (Article 14), privacy, and dignity (Article 21). These laws aim to curb cybercrimes involving non-consensual intimate imagery, but their effectiveness is limited by gaps in specificity and enforcement, particularly in tackling emerging technologies like deepfakes. Socio-legal analyses highlight how socio-cultural factors,

such as patriarchal norms and victim-blaming, exacerbate these challenges, undermining the legal response. This section examines the key provisions of the IT Act and IPC, their constitutional context, and their limitations in addressing revenge porn and deepfake pornography, providing a foundation for analyzing judicial interpretations and socio-cultural influences.

The Information Technology Act, 2000, addresses cybercrimes through Sections 66E, 67, and 67A, which penalize privacy violations, transmission of obscene material, and sexually explicit content, respectively, with penalties up to three years' imprisonment and fines. Section 66E targets non-consensual sharing of private images, while Sections 67 and 67A cover obscene or explicit content, potentially applicable to revenge porn. However, these provisions lack specific definitions for deepfake pornography, limiting their applicability to manipulated media. The IT Act also imposes intermediary liability under Section 79, as seen in Avnish Bajaj v. State (2005), but fails to address advanced technologies used in deepfakes, creating enforcement gaps.

The Indian Penal Code, 1860, complements the IT Act with Sections 354C (voyeurism), 509 (outraging a woman's modesty), and 292 (obscenity), which address non-consensual imagery and harassment, carrying penalties up to three years' imprisonment. Section 354C, introduced in 2013, criminalizes capturing or disseminating private images without consent, directly targeting revenge porn. Section 509 addresses acts insulting women's modesty, while Section 292 covers obscene content, but these provisions are outdated for deepfake technology, lacking specificity for synthetic media. Socio-legal studies note that these laws, while progressive, struggle to address the scale and anonymity of digital platforms.

The constitutional context underpins these laws, with Article 14 ensuring equality and Article 21 protecting privacy and dignity, as reinforced in Justice K.S. Puttaswamy v. Union of India (2017). Article 19(2) allows restrictions on free speech to protect public decency, supporting laws against obscene content. However, the undefined scope of deepfakes and the socio-cultural stigma around victims, particularly women, limit the laws' effectiveness, as victims face barriers in reporting due to shame and societal judgment.

The limitations of these laws include their lack of specific provisions for deepfake pornography and inadequate mechanisms to address online anonymity and rapid content dissemination. The next section will explore socio-cultural influences, analyzing how patriarchal norms and victim-blaming further complicate the legal response to these cybercrimes.

III. SOCIO-CULTURAL INFLUENCES ON REVENGE PORN AND DEEPFAKE PORNOGRAPHY

The proliferation of revenge porn and deepfake pornography in India is deeply intertwined with socio-cultural factors that exacerbate their prevalence and impact, complicating the enforcement of legal frameworks like the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860. Patriarchal norms, victim-blaming culture, and gender-based stigma shape societal attitudes toward these cybercrimes, disproportionately affecting women and undermining constitutional guarantees of equality (Article 14) and dignity (Article 21). Socio-legal analyses highlight how these cultural dynamics deter victims from seeking justice and amplify harm through digital platforms. This section examines the key socio-cultural influences—patriarchal norms and victim-blaming, the role of digital platforms and social media, and socio-economic factors like technology access and digital literacy—analyzing their impact on revenge porn and deepfake pornography and their implications for legal implementation.

Patriarchal norms and victim-blaming culture significantly drive the perpetuation of revenge porn and deepfake pornography, as they place disproportionate blame on women victims, discouraging reporting and prosecution. Indian society's patriarchal structure often views women's sexuality as a source of shame, leading to stigmatization of victims, as seen in cases where women face social ostracism for non-consensual imagery. Socio-legal studies note that this culture, rooted in gender inequality, aligns with dowry practices and son preference, further marginalizing women and violating Article 14's equality mandate. Victims hesitate to report due to fear of reputational damage, as highlighted in judicial discussions around Avnish Bajaj v. State (2005), where societal attitudes impacted legal recourse.

Digital platforms and social media amplify the harm of revenge porn and deepfake pornography by enabling rapid, anonymous dissemination of content. The accessibility of platforms like YouTube and early social media sites

facilitates the spread of non-consensual imagery, with perpetrators exploiting anonymity to evade accountability under IT Act Sections 66E and 67. Socio-legal analyses emphasize that online misogyny, rooted in cultural biases, fuels the creation and sharing of such content, targeting women to reinforce patriarchal control. The lack of robust platform accountability, despite intermediary liability under Section 79, exacerbates the issue, as platforms often fail to remove harmful content promptly, amplifying victims' trauma.

Socio-economic factors, including disparities in technology access and digital literacy, further complicate the issue. Rural and marginalized communities, with limited access to smartphones and internet, are less equipped to understand or combat cybercrimes, increasing vulnerability to exploitation. Conversely, urban populations with greater technology access face higher exposure to deepfake creation due to available tools, as socio-legal studies note. Low digital literacy among victims and law enforcement hinders effective use of IT Act provisions, while economic dependence on male family members discourages women from pursuing legal action, undermining Article 21's right to dignity.

These socio-cultural influences—patriarchal norms, digital platform dynamics, and socio-economic disparities—create significant barriers to addressing revenge porn and deepfake pornography, limiting the efficacy of legal frameworks. The next section will analyze judicial interpretations and their role in navigating these challenges to strengthen India's response to these cybercrimes.

IV. JUDICIAL INTERPRETATIONS AND THEIR ROLE

Judicial interpretations have been crucial in shaping India's response to revenge porn and deepfake pornography, navigating the legal framework provided by the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, while aligning with constitutional guarantees under Articles 14, 21, and 19(2). Courts have sought to address non-consensual intimate imagery, balancing victim protection with free speech and privacy rights, amidst socio-cultural challenges like patriarchal norms and victim-blaming. Socio-legal analyses highlight the judiciary's role in clarifying legal provisions and addressing enforcement gaps, yet limitations persist due to the lack of specific laws for deepfake technology. This section examines key judicial decisions, such as Avnish Bajaj v. State (2005), their limitations, and emerging trends in recognizing privacy and dignity under Article 21, analyzing their impact on combating these cybercrimes.

In Avnish Bajaj v. State (2005), the Delhi High Court addressed intermediary liability under Section 79 of the IT Act, involving the sale of a non-consensual intimate video on an online platform. The court clarified that intermediaries could face liability for failing to remove obscene content, aligning with Section 67 and Article 19(2)'s restrictions on free speech for public decency. This ruling set a precedent for holding platforms accountable, addressing socio-cultural issues like victim-blaming by emphasizing victim protection. However, the decision did not directly tackle deepfake technology, highlighting the IT Act's inadequacy in addressing manipulated media, a gap that limits judicial effectiveness in modern contexts.

Judicial limitations are evident in the absence of deepfake-specific precedents and inconsistent lower court rulings. While Avnish Bajaj addressed revenge porn, the judiciary has not yet fully grappled with deepfakes, which require advanced technical understanding beyond IPC Sections 354C (voyeurism) and 509 (outraging modesty). Socio-legal studies note that lower courts often fail to uniformly apply IT Act provisions, leading to delays and inadequate victim redress, as victims face societal stigma when pursuing justice. The lack of clarity on deepfake liability under existing laws restricts judicial ability to address emerging cybercrimes, undermining Article 21's protections for privacy and dignity.

Emerging judicial trends show increasing recognition of privacy and dignity as fundamental rights under Article 21, particularly for women victims. Courts have emphasized victim-centric approaches, as seen in cases involving non-consensual imagery, where Article 14's equality mandate is invoked to counter gender-based harm. The judiciary's focus on privacy, reinforced by broader interpretations of Article 21, signals a shift toward stronger protections against digital violations. However, without specific deepfake legislation, courts rely on outdated provisions, limiting their ability to address socio-cultural challenges like online misogyny and victim-blaming.

These judicial interpretations have advanced victim protections but are constrained by legal gaps and societal attitudes. The next section will explore legal gaps and enforcement challenges, analyzing how socio-cultural and technological barriers hinder India's response to revenge porn and deepfake pornography.

V. LEGAL GAPS AND ENFORCEMENT CHALLENGES

India's legal framework, encompassing the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, struggles to effectively address revenge porn and deepfake pornography due to significant legal gaps and enforcement challenges, exacerbated by socio-cultural and technological factors. Despite provisions like Sections 66E, 67, and 67A of the IT Act and Sections 354C and 509 of the IPC, the absence of specific laws targeting deepfake technology and non-consensual intimate imagery limits their efficacy. Socio-legal analyses highlight how patriarchal norms, victim-blaming, and rapid technological advancements complicate enforcement, undermining constitutional guarantees of equality (Article 14) and privacy (Article 21). This section examines key legal gaps, enforcement barriers, socio-cultural challenges, and technological issues, analyzing their impact on combating revenge porn and deepfake pornography in India's digital landscape.

The primary legal gap is the lack of specific provisions addressing deepfake pornography within the IT Act and IPC. Section 66E (privacy violation) and Sections 67 and 67A (obscene and explicit content) of the IT Act target general cybercrimes but fail to define or address manipulated media like deepfakes, as noted in socio-legal studies. Similarly, IPC Section 354C (voyeurism) criminalizes non-consensual imagery but is outdated for synthetic content, and Section 509 (outraging modesty) lacks precision for digital contexts. This absence of tailored legislation, as seen in Avnish Bajaj v. State (2005), limits judicial ability to prosecute deepfake cases, leaving victims without adequate recourse and undermining Article 21's privacy protections.

Enforcement barriers further hinder the legal response, with law enforcement agencies lacking technical expertise to investigate deepfake-related crimes. Socio-legal analyses point to inadequate training on cybercrime forensics, slowing investigations and prosecutions under IT Act provisions. The anonymity provided by digital platforms complicates identifying perpetrators, as platforms often fail to comply with intermediary liability under Section 79. Victim support systems are also limited, with few resources for counseling or legal aid, deterring reporting due to fear of societal judgment, particularly for women victims.

Socio-cultural barriers, rooted in patriarchal norms and victim-blaming, significantly impede enforcement. The stigma surrounding women's sexuality, as highlighted in socio-legal studies, discourages victims from reporting due to fear of social ostracism, reducing conviction rates under Sections 354C and 509. This culture, which often blames women for their victimization, undermines Article 14's equality mandate, perpetuating gender-based harm. Low reporting rates, coupled with societal pressure, weaken the legal framework's ability to deter offenders, allowing revenge porn and deepfake content to proliferate.

Technological challenges, driven by the rapid evolution of deepfake technology, outpace existing laws. The accessibility of tools to create manipulated media, combined with the viral nature of social media, amplifies harm, as seen in cases of non-consensual imagery dissemination. Platforms' inadequate content moderation, despite Section 79 obligations, exacerbates the issue, highlighting the need for technological interventions. The next section will provide a comparative analysis with international frameworks to identify solutions for addressing these legal and enforcement challenges.

VI. COMPARATIVE ANALYSIS WITH INTERNATIONAL FRAMEWORKS

India's legal framework for addressing revenge porn and deepfake pornography, primarily through the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, struggles with gaps in specificity and enforcement, compounded by socio-cultural challenges like patriarchal norms and victim-blaming. International frameworks offer valuable insights for addressing these issues, balancing victim protection with technological advancements. Socio-legal analyses underscore the need for India to adapt global best practices to strengthen its response to these cybercrimes, aligning with constitutional guarantees under Articles 14 and 21. This section examines the United Kingdom's Sexual

Offences Act, 2003, U.S. state-specific laws, and international standards like CEDAW, analyzing their approaches to non-consensual imagery and identifying lessons for India to enhance its legal framework.

The United Kingdom's Sexual Offences Act, 2003, provides a robust model for addressing revenge porn through specific provisions criminalizing non-consensual sharing of intimate images, with penalties up to seven years' imprisonment. Unlike India's IT Act Sections 66E and 67, which lack specificity for deepfakes, the UK law clearly defines offenses, facilitating prosecutions. The Act's victim-centric approach, supported by public awareness campaigns, reduces stigma, contrasting with India's socio-cultural barriers noted in cases like Avnish Bajaj v. State (2005). The UK's proactive policing and dedicated cybercrime units offer a blueprint for India to improve enforcement, ensuring compliance with Article 21's privacy protections.

In the United States, state-specific laws, such as California's revenge porn statute (Penal Code Section 647(j)(4)), criminalize non-consensual dissemination of intimate images with intent to harm, carrying penalties up to six months' imprisonment. While lacking federal deepfake legislation, states like New York have introduced bills targeting synthetic media. These laws emphasize victim consent and intent, unlike the broader IPC Section 354C (voyeurism), which struggles with deepfake contexts. U.S. frameworks, supported by advanced forensic capabilities, address technological challenges more effectively than India's under-resourced enforcement, offering lessons for aligning with Article 14's equality mandate by protecting victims equitably.

International standards, particularly CEDAW's Article 5, call for eliminating gender-based stereotypes, directly addressing India's socio-cultural issues of victim-blaming and misogyny. The UN's Beijing Platform for Action (1995) advocates for combating gender-based violence in digital spaces, providing a framework for India to counter online misogyny driving revenge porn. These standards emphasize victim support and public education, contrasting with India's limited counseling services, which deter reporting due to stigma. Adopting CEDAW's principles would strengthen India's response, ensuring gender equality and dignity under constitutional mandates.

Lessons for India include enacting specific legislation for revenge porn and deepfake pornography, inspired by the UK's clarity, and enhancing enforcement through trained cybercrime units, as in the U.S. Public awareness campaigns, aligned with CEDAW, can reduce stigma, while platform accountability measures can address technological challenges. The next section will propose reforms to address these legal gaps and socio-cultural barriers, fostering a robust framework for India's digital age.

VII. PROPOSED REFORMS AND STRATEGIES

India's legal framework, including the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, struggles to address revenge porn and deepfake pornography due to legal gaps, enforcement challenges, and socio-cultural barriers like patriarchal norms and victim-blaming. These issues undermine constitutional guarantees of equality (Article 14) and privacy (Article 21), necessitating comprehensive reforms. Socio-legal analyses highlight the need for specific legislation, enhanced enforcement, and public awareness to tackle these cybercrimes effectively. Drawing on international models like the UK's Sexual Offences Act, 2003, and CEDAW principles, this section proposes legislative reforms, strengthened enforcement mechanisms, public awareness campaigns, technological interventions, and alignment with international standards to foster a robust response to revenge porn and deepfake pornography in India's digital landscape.

Legislative reforms are critical to address the lack of specific provisions for deepfake pornography and revenge porn. Enacting a dedicated law, modeled on the UK's Sexual Offences Act, 2003, with clear definitions of non-consensual intimate imagery and synthetic media, would enhance prosecutions under Article 21's privacy protections. Amending the IT Act to include Section 66E provisions for deepfake technology and increasing penalties for Sections 67 and 67A violations would deter offenders. Similarly, updating IPC Section 354C (voyeurism) to cover manipulated content would address gaps noted in Avnish Bajaj v. State (2005), ensuring legal clarity and victim redress.

Strengthening enforcement requires specialized cybercrime units and training for law enforcement, addressing the technical expertise gap highlighted in socio-legal studies. Establishing dedicated units, as in the UK, to investigate digital offenses would improve prosecution rates under IT Act provisions. Enhancing victim support through

counseling and legal aid, as mandated by Article 21's dignity principle, would encourage reporting despite socio-cultural stigma. Regular audits of online platforms, enforcing intermediary liability under Section 79, would ensure swift removal of harmful content, reducing victim trauma.

Public awareness campaigns are essential to counter victim-blaming and gender stigma. Educational initiatives via media and community outreach should inform about legal protections under the IT Act and IPC, reducing societal shame, particularly for women victims. Collaborating with NGOs to conduct workshops on digital privacy and consent, as suggested by CEDAW's Article 5, would challenge patriarchal norms. These campaigns would empower victims to seek justice, addressing barriers noted in low reporting rates and aligning with Article 14's equality mandate.

Technological interventions, such as mandating platforms to deploy AI-based content moderation to detect deepfakes, would enhance accountability. Regulations requiring platforms to verify user identities for explicit content uploads, inspired by U.S. state practices, would curb anonymity-driven offenses. These measures would complement IT Act enforcement, addressing the rapid spread of non-consensual imagery on social media.

Aligning with international standards like CEDAW and the Beijing Platform for Action would strengthen India's framework. Incorporating CEDAW's focus on eliminating gender-based violence into domestic law would address socio-cultural biases, while adopting UN guidelines on digital safety would guide platform regulations. These reforms—legislative clarity, robust enforcement, awareness, and technological solutions—offer a comprehensive strategy. The next section will conclude the analysis, summarizing findings and outlining a future outlook.

VIII. CONCLUSION

India's legal framework, encompassing the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, seeks to address revenge porn and deepfake pornography but is hindered by significant legal gaps, enforcement challenges, and socio-cultural barriers like patriarchal norms and victim-blaming. These issues undermine constitutional guarantees of equality (Article 14) and privacy (Article 21), perpetuating harm, particularly to women victims. Judicial interpretations, such as Avnish Bajaj v. State (2005), have clarified intermediary liability and privacy rights, but the absence of specific provisions for deepfake technology limits their efficacy. Socio-legal analyses highlight that societal stigma and technological advancements exacerbate these challenges, with low reporting rates and inadequate enforcement allowing offenders to evade accountability. The comparative analysis with the UK's Sexual Offences Act, 2003, and CEDAW principles underscores the need for targeted legislation and victim-centric approaches. Proposed reforms—enacting specific laws for non-consensual imagery, strengthening cybercrime enforcement, launching awareness campaigns, implementing technological interventions, and aligning with international standards—offer a pathway to address these gaps. These measures aim to reduce stigma, enhance victim protection, and ensure platform accountability, aligning with constitutional mandates. The future of India's response to revenge porn and deepfake pornography depends on integrating legal reforms with cultural shifts, fostering a digital landscape that upholds dignity, equality, and justice for all.

REFERENCES

1. Avnish Bajaj v. State. (2005) 3 Comp LJ 364 Del.
2. Bandewar, Sunita. "Abortion Services and Providers' Perceptions: Gender Dimensions." Economic and Political Weekly, vol. 38, no. 21, 2003, pp. 2075-2081.
3. Basu, Durga Das. Shorter Constitution of India. 14th ed., LexisNexis, 2011.
4. Baxi, Upendra. "Abortion and the Law in India." Journal of the Indian Law Institute, vol. 28-29, 1986-87, pp. 28-29.
5. Berlatsky, Noah. Abortion. Greenhaven Press, 2011.
6. Centre for Enquiry into Health and Allied Themes (CEHAT) v. Union of India. (2001) 5 SCC 577.
7. Chitnis, Varsha, and Danaya Wright. "The Legacy of Colonialism: Law and Women's Rights in India." Washington & Lee Law Review, vol. 64, no. 4, 2007, pp. 1315-1348.
8. Constitution of India, 1950. Government of India, 1950.
9. D. Rajeshwari v. State of Tamil Nadu. 1996 Cri LJ 3795.
10. Dr. Nikhil Dattar v. Union of India. Writ Petition No. 1816 of 2008, Bombay High Court, 2008.

11. Gaur, K.D. "Cyber Laws in India: An Overview." Journal of the Indian Law Institute, vol. 49, no. 2, 2007, pp. 201-220.
12. Government of India. Census of India 2001: Sex Ratio. Office of the Registrar General & Census Commissioner, 2001.
13. Indian Penal Code, 1860. Government of India, 1860.
14. Information Technology Act, 2000. Government of India, 2000.
15. Jain, M.P. Indian Constitutional Law. 6th ed., LexisNexis Butterworths, 2011.
16. Jaiswal, J.V.N. Legal Aspects of Pregnancy, Delivery, and Abortion. Eastern Book Company, 2009.
17. Jesani, Amar, and Aditi Iyer. "Women and Abortion." Economic and Political Weekly, vol. 27, no. 46, 1992, pp. 2467-2470.
18. Kamdar, Mira. Cyberlaw in India. Universal Law Publishing, 2009.
19. Medical Termination of Pregnancy Act, 1971. Government of India, 1971.
20. Medical Termination of Pregnancy (Amendment) Act, 2002. Government of India, 2002.
21. Murari Mohan Koley v. The State. 2003 Cri LJ 1482.
22. National Crime Records Bureau. Crime in India 2010. Ministry of Home Affairs, Government of India, 2010.
23. Paranjape, V.N. Indian Penal Code. Central Law Publications, 2010.
24. Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 2002. Government of India, 2002.

INTERNATIONAL JOURNAL OF

MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY