INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 3 [2025] | Page 509 – 519

DIGITAL PRIVACY AT RISK: "EXAMINING INDIA'S LEGAL RESPONSE TO THE NON-CONSENSUAL SHARING OF INTIMATE MEDIA"

- Priyanka Kumari[1]

-Sukriti Chaudhary[2]

-Madhurima Das[3]

ABSTRACT

The rapid rise of digital platforms has made it all too easy for non-consensual sharing of intimate media to occur, putting victims especially women at a risk of serious psychological, reputational, and legal damage. Even though the right to privacy was acknowledged in the case of K.S. Puttaswamy v Union of India, the legal framework in India is still quite fragmented and largely ineffective when it comes to tackling image-based abuse. Current laws under the Information Technology Act 2000, the Indian Penal Code, and the Digital Personal Data Protection Act 2023 fall short in addressing new threats like deepfakes and AI-generated content. This paper takes a close look at the socio-legal gaps surrounding non-consensual intimate content in India, using doctrinal analysis, case studies, and comparative perspectives. It draws on the work of scholars like Sharma, Halder, and Basu to highlight the institutional and cultural hurdles that make it difficult to seek justice, such as patriarchal attitudes in law enforcement, inconsistent responses from platforms, and a lack of victim-focused solutions. The study suggests that legislative reform is needed, advocating for a unified, gender-neutral offense, increased responsibilities for platforms, and educational outreach. Ultimately, it argues that without proactive and coordinated legal measures, violations of digital privacy will continue to disproportionately affect marginalized voices in India's digital landscape.

Keywords: Non-consensual intimate media, deepfakes, digital privacy, image-based abuse, legal reform.

[1] 3rd Year, Student at National University of Study and Research in Law, Ranchi

[2] 3rd Year, Student at National University of Study and Research in Law, Ranchi

[3] 3rd Year, Student at National University of Study and Research in Law, Ranchi

CHAPTER 1. INTRODUCTION

"ONE CLICK CAN BREAK A LIFETIME"

This harsh reality highlights the overwhelming susceptibility of Indian citizens in a rapidly digital age. More recent scholarship by Sharma describes a fractured legal landscape that does not adequately treat non-consensual intimate image sharing as a discrete offence, offering victims diffuse and generally delayed redress.[4] Building on this critique, Halder and Basu contend that image-based harassment moves beyond jejune "revenge-porn" stereotypes to represent a more comprehensive form of gender-based violence which is technologically advanced and embedded in patriarchal relations.[5]

India's phenomenal transition to the digital age defined by low data costs and pervasive smartphone penetration has inadvertently created fertile ground for privacy breaches. Intimate photographs, previously private, can now be duplicated, manipulated and profited from over anonymous platforms within seconds. The impact on the victim is catastrophic: consisting not only of emotional distress but reputation damage, economic extortion and deep-seated social stigma.[6]

Even with several statutory provisions like sections 66E and 67A of the Information Technology Act 2000, and voyeurism offenses under the IPC available to it, the legal response is still reactive in nature. Judicial interventions like takedown orders and interim reliefs often get mired in jurisdictional silos, dispersed enforcement, and the platform-based obscurity that Halder and Basu identify.[7] Such legal patchwork sets important questions: Do existing Indian legislations sufficiently address the extent and magnitude of intimate image-based harassment? And what are the socio-legal dynamics that aggravate or mitigate its harms?

This paper attempts to resolve these questions through a critical examination of statutory instruments, judicial trends, and platform obligations in the Indian context. It synthesizes doctrinal legal analysis, case law examination, and stakeholder interviews to set forth an enriched legal framework, one that is victim-focused, gender-neutral, and reflective of digital consent. In

[4] Sharma ('title…') (2022) NLUJ Sl Review, p X.
[5] Halder and Basu, *Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India* (2024) *Information & Communications Technology Law* https://www.tandfonline.com/doi/full/10.1080/13600834.2024.2408914#d1e120
[6] Ibid
[7] Ibid

comparative perspective and drawing from Indian law and lived reality, this research hopes to chart a revolutionized future for digital privacy and dignity in India.

CHAPTER 2. CONCEPTUAL FOUNDATIONS

Non-consensual dissemination of intimate images, often referred to as "NCII," is all about sharing private and intimate media like nude or sexually suggestive photos and videos without the person's consent. This holds true even if the content was initially captured with consent. This type of digital violation falls under a larger umbrella known as image-based harassment, which includes things like unauthorized sharing, malicious exposure, cyberbullying, and even non-consensually created synthetic sexual media, such as deepfakes.[8]

Deepfakes, which are fake images or videos made using AI, present a serious risk because they can show people in intimate or sexual situations without their consent, often in a misleading way. Voyeurism, on the other hand, involves secretly capturing intimate images without someone knowing or agreeing to it, think hidden cameras in bathrooms or bedrooms and these images are often shared without permission. Lastly, sextortion is a coercive tactic where someone threatens to release intimate content unless the victim meets certain demands, like sending more images, paying money, or performing specific acts.

Sharma's analysis highlights that India's current legal system where a confusing mix of the IT Act, IPC, voyeurism laws, and data protection rules doesn't adequately tackle these complex issues of intimate content abuse, especially when it comes to non-consensual sharing, deepfakes, and sextortion.[9] Meanwhile, Halder and Basu advocate for a rethinking of these various harms under the concept of image-based abuse, emphasizing that a victim-focused definition is crucial to ensure that laws keep pace with the changing landscape of digital gendered violence.[10]

3. LEGAL FRAMEWORK AND LIMITATIONS

India's legal framework for tackling the non-consensual sharing of intimate media is quite fragmented and tends to react rather than proactively address the issue, hampered by structural and enforcement shortcomings. The Information Technology Act of 2000 includes Section 66E, which makes it a crime to intentionally capture, publish, or share private images without consent,

[8] Non-consensual image-based abuse, including deepfakes, voyeurism and sextortion, defined in *Non-Consensual Sharing of Intimate Images*, Media Defence Module 2 (2023). https://www.mediadefence.org/ereader/publications/online-violence-against-journalists/module-2-digital-attacks-and-online-gbv/ncii/?tztc=1

[9] P Sharma, 'Understanding non-consensual dissemination of intimate images …' (2022) *NUJS Law Review*. https://nujslawreview.org/wp-content/uploads/2022/03/14.4-Sharma-1.pdf

[10] Supra Note 2

with penalties of up to three years in prison or a fine of ₹200,000.[11] Section 67A takes it a step further by punishing the electronic transmission of sexually explicit content, with potential imprisonment of up to seven years and fines that can reach ₹1 million.[12] While these laws represent some progress, they fall short in being proactive lacking essential measures like mandatory hash-matching by platforms, quick takedown requirements, or clear timelines making them inadequate in the face of the fast and anonymous spread of digital content.

The Indian Penal Code, along with its successor, the Bharatiya Nyaya Sanhita, includes Section 354C, which addresses voyeurism specifically, watching or recording a woman in a private act or sharing such images.[13] This law imposes a prison sentence of one to three years for a first offence and three to seven years for repeat offenders. However, its definition is quite narrow: it only applies to women, pertains to activities deemed "private" (like using a restroom or changing clothes), and does not cover recordings made in public spaces or digitally altered content. Judicial interpretations have further limited its effectiveness by ruling that recordings made in public do not fall under the category of "private acts," which weakens the law's impact.[14]

The Digital Personal Data Protection Act of 2023 brings in significant rights, such as the ability to erase data and withdraw consent, which could empower victims to request the removal of intimate content.[15] However, the practical application of these rights is still minimal, largely due to a lack of awareness among the public and institutions, as well as the early stage of enforcement mechanisms like the Data Protection Board. So, even though privacy rights are recognized in theory, the reality is that they often remain unfulfilled.

3.1 LEGISLATIVE SILENCE ON DEEPFAKES AND AI-GENERATED CONTENT

Legislative Silence on Deepfakes and AI-Generated Content Right now, India doesn't have any specific laws to tackle the rising issue of deepfakes, those synthetic media pieces created by artificial intelligence that often show people in intimate or compromising situations without their consent.[16] While Section 67A of the Information Technology Act 2000 could be used for sexually explicit content, it doesn't really address manipulated or fake content directly. This gap in legislation is particularly alarming, especially since deepfakes have been increasingly used to harass women,

[11] *Information Technology Act 2000*, s 66E.
[12] Ibid, s 67A
[13] *Indian Penal Code* s 354C (as inserted by Criminal Law (Amendment) Act 2013)
[14] Devgan, IPC Section 354C (voyeurism) (visited 19 June 2025) https://devgan.in/ipc/section/354C/
[15] Digital Personal Data Protection Act 2023, s 12.
[16] *Information Technology Act 2000,* s 67A

celebrities, and those who speak out against the government. Halder and Basu point out that without clear legal recognition, victims of this kind of synthetic media abuse are left to deal with confusing legal situations, where intent and "authenticity" are often up for debate.[17] This highlights an urgent need to update Indian cyber law by adding specific offenses related to AI and banning content manipulation.

3.2 THE ROLE OF INTERMEDIARIES AND THE IT RULES, 2021

The *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021* were introduced to enhance platform accountability. Rule 3(1)(d) mandates that intermediaries remove unlawful content within 36 hours of notification.[18] Rule 4 imposes obligations on significant social media intermediaries to enable traceability and deploy automated tools for detecting harmful content. However, the enforcement of these rules remains inconsistent, and their constitutional validity is currently under challenge for overreach and privacy violations.[2] Sharma critiques these rules as "regulatory theatre," suggesting that without robust monitoring and penal consequences, platforms have little incentive to act swiftly or transparently.[19]

3.3 CHALLENGES IN REPORTING AND ACCESS TO REMEDIES

One of the biggest challenges to dealing with non-consensual sharing of intimate images in India is that there are no readily available and efficient redressal mechanisms for victims. Most victims are not aware of the legal avenues available to them, e.g., online reporting platforms like the National Cybercrime Reporting Portal or even through local police stations.[20] The situation is also worsened by a lack of awareness regarding which provisions of law are applicable, whether the Information Technology Act, Indian Penal Code, or the Digital Personal Data Protection Act. Even after registering complaints, police officers tend to downplay the damage, seeing such acts as "private affairs" or blaming the victim for producing the content to begin with.[21] Such attitudes not only deter victims from seeking justice but also lead to inappropriate registration of First Information Reports (FIRs), misuse of legal provisions, or refusal to act in extremis.

Sharma rightly describes this as an "offline bias" among police where officers who have mostly been trained to deal with physical crimes are short on technological expertise or empathy when it comes to dealing with online privacy violations.[22] Police stations themselves are often not well-

[17] Supra Note 2
[18] *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021,* r 3(1)(d).
[19] Supra Note 6
[20] S Choudhury, *Women and Cyber Harassment in India* (OUP 2020) 89.
[21] LawSchoolPolicyReview.com, 'Structural Patriarchy in Cyber Crime Cells' (2024)
[22] Supra Note 6

equipped to perform necessary digital forensic activities, e.g., tracing IP addresses, extracting information from intermediaries, or issuing timely takedown notices. The lack of standardised procedures and mechanisms for digital evidence preservation adds to the problem.[23] Furthermore, victim-friendly infrastructure like female cybercrime officers, psychological support units, or confidential complaint systems is scarce or non-existent in most jurisdictions.[24] As a consequence, delayed intervention ensues, excessive exposure of sensitive material online occurs, and psychological trauma for victims arises. Unless reporting mechanisms are streamlined, digitized, and victim-focused, supported by frequent training of law enforcers, legal safeguards will be theoretical and not practical for many of the affected parties.

3.4 NEED FOR A STANDALONE LEGISLATION ON IMAGE-BASED ABUSE

Despite rising instances of intimate image abuse, India has yet to introduce a standalone statute explicitly addressing image-based sexual abuse. Most other jurisdictions including the UK, Canada, and Australia have legislated dedicated offences that are gender-neutral, cover synthetic content, and include speedy takedown obligations.[25] Indian legislation continues to treat such offences as offshoots of voyeurism, obscenity, or data protection violations, lacking the specificity required to address evolving forms of abuse. Scholars argue that a comprehensive law should not only criminalise the act but also lay down mechanisms for immediate redressal, mandatory takedown, compensation, and psychological counselling.[26]

CHAPTER 4. CASE STUDIES AND JUDICIAL TRENDS

Vaishnavi Sharma's comprehensive study highlights the chronic underdevelopment of India's legal response to non-consensual intimate image dissemination. It critiques the law's reactionary stance fragmented provisions under the IT Act and IPC are sporadically applied, rarely integrated into a cohesive framework, and focused on punishment rather than prevention or victim support.[27] Similarly, the work accessible via ePrints at White Rose University analyses prominent incidents such as the Ritu Kohli, Rana Ayub, 'Sulli Deals' and Rashmika Mandanna deepfake cases, depicting

[23] P Sinha, 'Policing Online Abuse in India: Technology Gaps and Institutional Constraints' (2023) 9 Indian Journal of Cyber Law 56. https://bprd.nic.in/uploads/pdf/IPJ%20Book-1-4-25%20Final.pdf
[24] Centre for Internet and Society, 'Cybercrime and Women in India: Challenges and Recommendations' (2022).
[25] Clare McGlynn and Erika Rackley, 'The Criminal Law's Response to Image-Based Sexual Abuse' (2017) 80 MLR 26. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874136
[26] D Halder and S Jaishankar, *Cyber Crimes Against Women in India* (Sage Publications 2021).
[27] Supra Note 2

the changing nature of digital image-based harm.[28] These cases encompass everything from misogynistic objectification and non-consensual exposure to sophisticated AI-driven deepfakes, underscoring how existing legal categories fail to fully capture evolving forms of digital violence.

Judicial responses have been more proactive in recent years. In *Mrs X v Union of India*, the Delhi High Court invoked its writ jurisdiction to order prompt takedown of non-consensual intimate images, directed intermediaries to deploy hash-matching for preventing reposting, and mandated that the National Cybercrime Reporting Portal include status tracking and round-the-clock grievance redressal procedures.[29] This judgment also instructed police to file FIRs immediately upon complaint and uphold the victim's "right to be forgotten" as part of the broader right to informational privacy.[30]Complementing this, courts have granted interim relief such as URL-blocking orders against search engines and social media platforms—and in some instances awarded compensation to victims for violation of privacy and reputational harm.

Though these judicial trends signal an encouraging departure from inertia, enforcement remains inconsistent. Constitutional writs are limited by jurisdiction, and hash-based removal is still nascent in India. Taken together, these developments reveal a legal landscape in flux—pockets of judicial innovation striving to compensate for systemic inertia, yet constrained by narrow laws, limited enforcement tools, and the absence of a unified offence for non-consensual intimate image dissemination. It remains clear that without comprehensive statutory reform, judicial mechanisms alone cannot keep pace with emerging online harms.

CHAPTER 5. SOCIO-LEGAL DYNAMICS

Platform dynamics have presented considerable challenges to instant justice in instances of non-consensual intimate media sharing. Halder and Basu decry big social media companies for their passive approach: "delay and opacity" usually characterize their takedown processes, and through them, victims are kept exposed and harmed for excessively long periods.[31] People often complain about experiencing long wait times before content is taken down, with hardly any transparency in decision-making or escalation mechanisms. Such inertia not only worsens

[28] See ePrints@University of York, 'Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India' (Halder & Basu, 2024) https://eprints.whiterose.ac.uk/id/eprint/217778/7/Digital%20dichotomies%20%20navigating%20non-consensual%20image-based%20harassment%20and%20legal%20challenges%20in%20India.pdf
[29] *Mrs X v Union of India* 2023:DHC:2806 https://indiankanoon.org/doc/105980506/
[30] Ibid Delhi HC
[31] Supra Note 6

psychological suffering but also indicates a wider regulatory vacuum in holding platforms to account.

Its effect on the victims, particularly women, is both instant and long-lasting. Research indicates that victims of image-based abuse suffer from serious psychological trauma, reputational harm, and extreme social ostracism.[32] In the case studies of incidents like those involving Hassan and Karavali MMS, some victims lost employment, were evicted, and even tried to commit suicide because of the extreme personal consequences.[33] A close inspection of policy cases in law also shows the way reputational damage mediates chronic social exclusion and emotional suffering, especially where violations of intimacy meet highly ingrained stigma.[34]

These discrete harms are supplemented by the larger cultural environment in which they take place. Patriarchal attitudes deeply ingrained in society and institutions still shape societal and institutional reactions to privacy invasions. Women are typically considered bearers of family honour and over-represented as the cause of the transmission of intimate media.[35] This is symptomatic of a broader pattern under which patriarchal norms support low reporting levels, victim-blaming, and institutional disregard—particularly in law enforcement and judicial proceedings.[36] The socialization that women must be invisible and promote modesty only further deepens their exposure to digital rights abuses, placing both cultural reform and legal reform on an urgent agenda.[37]

CHAPTER 6. COMPARATIVE PERSPECTIVES & BEST PRACTICES

In analysing India's piecemeal approach to the non-consensual sharing of intimate images, comparative legal systems provide useful insights into best and victim-protective practices. Sharma draws attention to the importance for India to look towards regimes like that of the United Kingdom, under which the sharing of intimate sexual images and movies without consent is

[32] *The Crying Shame of Image-Based Abuse* (Factor Daily, 2024) https://factordaily.com/the-crying-shame-of-image-based-abuse/
[33] ibid
[34] LawSchoolPolicyReview.com, 'Psychological trauma and reputational damage' (visited 19 Jun 2025)
[35] Frontiers, *A global study into Indian women's experiences of domestic violence and control* (2024) https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2024.1273401/full
[36] Indian Express, 'Patriarchy and violence against women' (2025) https://indianexpress.com/article/upsc-current-affairs/upsc-essentials/patriarchy-and-violence-against-women-9587478/
[37] Frontiers, *Trivialization of aggression against women in India* (2022) https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.923753/full

criminalised by the Criminal Justice and Courts Act 2015.[38] The UK legislation is significant not merely because of its gender-neutral drafting and concise definitional scope but also because it encompasses malicious intent and psychological harm as aggravating factors. In addition, the application of hash-based detection and removal technologies, driven by organisations including the Internet Watch Foundation that has assisted in limiting the spread of malicious material across platforms.[39] These forward-looking tools are a far cry from India's reliance on post-incident response.

Halder and Basu also promote policy harmonisation on the international level to confront the very borderless character of cyber abuse.[40] Australia and Canada, among other nations, have enacted precise legislation addressing image-based sexual abuse and commonly supported by civil relief, privacy commissioners, and rapid takedown regimes.[41] Australia, for instance, introduced the Enhancing Online Safety Act 2015 that created an eSafety Commissioner through which victims may seek quick takedown of intimate content from social media, apps, and websites.[42] Canada's Protecting Canadians from Online Crime Act criminalises the non-consensual sharing of intimate images and allows courts to impose restraining orders and compensation.

Conversely, India's dispersed statutory framework and divergent judicial strategies rely heavily on victims for enforcement. By incorporating the best from these jurisdictions especially legislative precision, platform responsibility, and administrative remedy mechanisms, India can build a stronger and more responsive legal system. The comparative perspective then underscores the imperative of statutory unity and institutional creativity over depending on the altruism of courts or piecemeal enforcement

CHAPTER 7. RECOMMENDATIONS

In order to adequately respond to the non-consensual sharing of intimate images, a multi-faceted legal, institutional, and societal reform approach is necessary. **First**, India needs to enact a specific, gender-neutral criminal offense clearly defining and punishing the unauthorized production, sharing, or tampering with intimate content, including synthetic material like deepfakes.[43] The

[38] *Criminal Justice and Courts Act 2015* (UK), s 33
[39] Internet Watch Foundation, 'Annual Report 2023' https://www.iwf.org.uk
[40] Supra 2
[41] Clare McGlynn, Erika Rackley and Ruth Houghton, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25(1) *Feminist Legal Studies* 25
[42] *Enhancing Online Safety Act 2015* (Cth), ss 7–10 (Australia)
[43] Supra Note 38

current provisions under the Information Technology Act 2000 and the Indian Penal Code are inadequately framed and piecemeal, rendering prosecution time-consuming and uneven.[44] Statutory reform hence needs to broaden the IT Act to comprehensively cover offenses involving image-based abuse, especially deepfake technology and non-consensual material created using the technology.[45]

Second, more robust platform responsibility is acutely needed. Social media and content-hosting intermediaries must be required to deploy proactive detection mechanisms such as hash-matching technologies and to act on takedown notices within legally specified time periods. Transparency reports must also be compulsory, reporting action taken against reported content and response times.[46] **Third**, the rights-based approach under the Digital Personal Data Protection Act 2023 must be used, utilizing its erasure and consent-withdrawal provisions for intimate content violations. Victims must be able to initiate removal of such content on all platforms without tedious procedural hurdles.[47]

No less critical are institutional and societal reforms. There is an imperative need for legal literacy courses and online training of law enforcement officers, many of whom do not have the sensitivity and technical knowledge needed to deal with these cases.[48] Awareness campaigns and digital safety education at schools can create early comprehension of consent and online harm, while workplace empowerment initiatives can build organisational responses to cyberbullying.[49] These reforms combined will address the current legal and enforcement loopholes and provide a responsive, humane, and technologically advanced remedy framework to the unfortunate victims.

CHAPTER 8. CONCLUSION

The unauthorized sharing of private media is one of the most serious breaches of digital privacy and personal dignity we face today. This study highlights that victims mostly women often endure lasting psychological harm, damage to their reputations, and social isolation. While Indian laws like the Information Technology Act 2000, the Indian Penal Code, and the Digital Personal Data Protection Act 2023 provide some options for recourse, they still fall short, being fragmented, reactive, and outdated in terms of technology. These laws don't offer comprehensive, victim-

[44] Supra Note 6
[45] Supra Note 2
[46] Supra Note 38
[47] Supra Note 12
[48] Supra note 22
[49] LawSchoolPolicyReview.com, 'From Awareness to Action: Strengthening Digital Literacy for Gendered Online Abuse' (2024)

focused solutions, especially when it comes to new challenges like deepfakes and synthetic sexual content. Judicial efforts have sometimes tried to bridge this gap by providing temporary relief and takedown orders, but these initiatives are often hindered by unclear jurisdiction, slow enforcement, and non-compliance from platforms. Without a clear and unified legal definition that recognizes and criminalizes the non-consensual sharing of intimate images regardless of the victim's gender or the content's nature. true accountability will remain out of reach.

To move forward, we need to build a solid legal framework that is gender-neutral, adaptable to technological changes, and focused on protecting informational privacy. Legislative clarity should go hand in hand with ongoing judicial education and strengthening the capabilities of law enforcement agencies. At the same time, digital platforms must be held to higher standards of accountability through automated detection tools, timely takedown requirements, and transparent reporting systems. Only by creating a comprehensive and coordinated approach can we effectively safeguard the privacy, autonomy, and dignity of individuals in India's rapidly changing digital landscape.