Revenge Porn as an Emerging Form of Gender-Based Cybercrime and Adequacy of Indian Legal Framework in the Digital Age

[1] Esha Anand, [2] Dr. Tarun Kaushik
[1]Research Scholar, Sharda School of Law
Sharda University, Greater Noida, India
Email ID- eshaanand890@gmail.com
[2]Assistant Professor, Sharda School of Law
Sharda University, Greater Noida, India
Email ID- tarun.kaushik@sharda.ac.in

Abstract
Non-consent intimate image abuse, a revenge porn is a pernicious form of gender-based cyber-crime, characteristic of using digital platforms to compromise the privacy, dignity, and autonomy of women violatively. It is one of the trends in the digital era of India that have begun to rise dominantly, and it entails the deliberate sharing of intimate pictures or videos without permission, most of the time done by ex-lovers seeking revenge or extortion, and even humiliation. Such behaviour has devastating psychological trauma, social ostracism, reputational damage, and secondary victimisation. It is defined as the virtual rape, whereby scholars and activists characterise its continuation to enable the perpetuation of patriarchal control by virtue of the violence that is implemented through technology. Non-consensual intimate image abuse (NCII) or image-based sexual abuse (IBSA) of individuals is an emerging and devastating gender-based cybercrime that is widespread and prevalent in the modern Indian society. This is a type of premeditated sharing, uploading, or distribution of intimate photographs, videos, or morphed images without the permission of the subject, which is usually carried out by former partners, friends, or bad people who may want to seek revenge, blackmail, control, or humiliate.

Keywords: Revenge porn, Gender-based cybercrime, Indian legal framework, Information Technology Act, Digital Personal Data Protection Act

1. Introduction

The practice is not a privacy infringement but causes irreparable long-term damage akin to sexual violence and is often discussed in feminist law circles as a form of rape of one of a virtual kind. Objectifying the victims, eliminating their free will, and causing severe psychological trauma (such as anxiety, depression, and even suicidal thoughts), it creates social stigma, loss of work, family rejection, and secondary revictimisation via online shaming or doxxiing. These abuses become particularly strongly felt in the digital ecosystem of India, which is patriarchal: smartphone penetration and social-media use in India have skyrocketed, with women bearing the brunt of such abuses, evidenced by a consistently rising number of incidents associated with relationship breakdowns, sextortion, and, most recently, deep-faked manipulations through artificial-intelligence technologies.

The Indian legal reaction, though enlightened in certain ways, is disjointed and unable to carry out the entire coverage of the changing threat in the digital age. An Information Technology Act, 2000 (amended 2008) becomes the foundation, especially the intentional capture, publication or transmission of a photograph of the private areas of a person against the will of the person, which is punishable by up to three years of imprisonment and/or a fine of 2 lakh rupees is considered a breach of privacy (via Section 66E). Strictly speaking, sections 67 and 67A deal with obscene and sexually explicit electronic material, and so it captures technological transmission and publication to a greater extent. The live law Bharatiya Nyaya Sanhita, 2023 (albeit ineffective until 2024 and replacing the IPC), also retains and elaborates at

least one such provision voyeurism (Section 77, now gender-neutral in certain contexts, although confined to capture and not distribution), stalking, sexual harassment, and insult to modesty. The Digital Personal Data Protection Act of 2023 (DPDP Act) proposes the rights to consent withdrawal, data erasure, and fiduciary accountability thus possibly enabling victims to request the content-of-infringement be removed. Guidelines in the IT Rules, 2021, involve due diligence on the material that platforms must remove at short notice on complaint.

Irrespective of these provisions, there exist major holes which lead to lack of efficacy. There is no specific law criminalising or defining revenge porn or NCII as a distinct gender-specific crime revolving around consent infringement and sexualised violence; it has to be pieced together in individual bits through obscenity, voyeurism or privacy provisions and thus water downs intent and impact. The provisions of voyeurism, such as, are concerned more with acquisition at the inception, than mass sharing at the downstream or the endless availability on the internet. Obscenity segments at the expense of victim-shaming by comparing consensual self-representation with criminality, which creates a chilling effect on coverage. Challenges to implementation are rampant: proving intent is tricky, tracing an anonymous upload is tricky, police are prone to resistance, judicial slow-moving, low conviction rates, and lack of reliability with hosting the company despite regulation requirements. Celebrity decisions, including those of the State in v. West Bengal, 2018. The cases of Animesh Boxi, who was sentenced to five years of imprisonment and a fine due to uploading of intimate photographs belonging to an ex-partner, show judicial ingenuity, such as compensatory treatment of victims as other rape survivors, but reveal inconsistencies in the systems and the lack of quick and survivor-centered solutions.

New issues increase these gaps. The generation of synthetic intimate content through the use of AI-generated deepfakes offers a way around any small delimits of the definition of the intimate area and capture in current laws. The spread of metaverses and virtual states opens new channels of abuse, and failures in content control across the platforms on a global scale only continue the damages. The comparative study of scenes as the United Kingdom, the Philippines, and some member states of the European Union also demonstrate that particular NCII pertinent laws, with the focus on being expressly consented to, not subject to bail, and civilized with recourse to courts, offer good lessons to India.

2. Revenge Porn: Definitions, Typologies, and Socio-Psychological Dimensions

The term revenge porn which originated in the early 2000s to describe the online websites that assist the unconsented dissemination of intimate photographs, usually of women, with personal identities and excuses of the act of so-called revenge, has been subtly refined. The word initially gave the thrust a retaliatory lintel, permitting that the content had been uploaded by former companions or other individuals as a way of humiliation or punishment. Nevertheless, this nomenclature has been widely criticised by academics, survivor-advocacy and professional organisations, who believe that it creates an impression of victim culpability by suggesting that the person who is is exposed was a transgressor, limits itself to revenge-related cases and fails to acknowledge a wide range of perpetrator motives, including sexual gratification, boasting, extortion, or coercion and confuses non-consensual intimate imagery with commercial pornography, thus devaluing the abuse. Survivor centred words have therefore become rather common. The term non-consensual intimate image abuse (NCII) or non-consensual intimate imagery presupposes the missing continuatory, express consent at the creation, distribution, or threat of these stages. This generalized category of exploitative behaviour, Jesus-Image Economic Sexual Abuse (ibsa) as introduced by UK researchers (and popularised by Clarein the 00s and Erikain the 10s) covers a wider range of exploitative acts, including non-consensual production, sharing or threating by force to send intimate images or video. The IBSA predicts the sexualised nature of the harm, the gendered processes, and the use of technology that enabled the violation, hence closer to what is already established as the sexual violence forms of this violence as opposed to a simple categorisation of pornography. This change is characteristic of feminist criminological practices that refuse the victim-blaming discourse and find IBSA to form a spectrum of gender-based violence.

The types and forms of this abuse have grown across the Internet infrastructure and no longer comprise primitive sharing, but now are the technical exploiter of technologies. Revenge porn began first as the unwanted sharing of self-created or consensually shared intimate photographs (e.g. nudes sent in a state of trust within a relationship) through social media, messaging applications, pornographic websites or specially designed revenge forums. Such posts are often accompanied with doxxing, the public distribution of the names, addresses, work or contact details of the victims, to increase harassment and to present a real threat to their beings. Downstream diffusion also creates a false sense of permanency: once uploaded, an image virally disperses across it as it transfers across platforms, forums, even the darkest, and darkest of peer networks, resurfacing even after takedown requests. Modern modalities encompass voyeuristic capture using undercover cameras or upskirting/downblousing, sextortion by use of threats of exposure on compliance, and forced sexting whereby one is forced to create or spread images. Artificial-intelligence-based inventions have also produced deepfakes artificial media products that combine face-related features onto pornographic figures using generative adversarial networks (GANs) or morphing or nudification applications that digitally manipulate clothed photographs into the form of nude or sexually explicit bodies. These fake content are often not recognizable as fake, and they extend the range of abuse, not only to non-intimate acquaintances, celebrities, and even children (morphed child sexual abuse material). The unsolicited sharing, also known as cyberflashing, and forced production are additional diversification of modalities that appear in such situations as intimate partner violence (IPV), cyberbullying, large-scale cybercrime, or a series of harassment campaigns. The digital virtual technologies work relentlessly to improve the disseminability of the network, digital affordances privacy, end-to-end automation, cross-platform as permanence, turn single uses into a chain reaction, and turn an unattained act into a persistent year-long transgression.

Fundamentally, revenge porn, IBSA, and NCII are deeply gendered and, more fundamentally, they are patriarchal power sources and control, objectification, and domination over women. Women and girls are also most frequently victimised, both worldwide and in India, they were found by both global and Indian research to make up the vast majority of reported cases, and they frequently are the victims of men, including their former partners, friends, or strangers. This imbalance is reinforced by deeply ingrained gender beliefs which are more harsh in policing the feminine sexuality and autonomy over their bodies compared to the male gender in which the sexual discretion of females is perceived as deviant or punishable. Using intimate imagery, perpetrators reinvert the dominance of femininity: punishing perceived transgression (e.g., breaking up relationships, turning down advances), demand of independence, and slut-shaming and character attack. The sexualisation forced on the victims serves to dehumanize them, therefore, reinvesting in male privilege and inferiority of women, both in intimate (e.g., IPV pressure) and in official domains.

Cultural demands of modesty in patriarchal cultures like India further heighten the levels of stigma attached to them: the victims face the burden of rejection by their families, ostracism by society, reduced chances of marriage, occupational discrimination, and community disapproval, often internalising the resultant discomfort as shame. The effects are psychologically similar to those of sexual assault trauma, including disenfranchisement of the body, trust disdain, and unstopping re-victimation with the resonance of the images. High scores of anxiety, post-traumatic stress disorder (PTSD), suicidal ideation, low self-esteem, mistrust especially in intimate relationships, hypervigilance and social withdrawal are disclosed by survivors. Secondary victimisation adds to the injury: victim-blaming by the police, or family relations or social networking (e.g., asking questions like why did you send the picture?), redistributes blame to the victim again, reinforcing the longstanding dynamics of rape-culture. The long-term consequences are permanent shame, self fragmentation, and shading away of online intimacy.

IBSA continues to perpetuate the culture of rape by making technological-enabled sexual violence a normal response to the agency of women, which strengthens the patriarchal structures by reinforcing the

works of fear, silence and control. To combat this and not regard it as an individual deviance but gendered cybercrime on a systemic level, interventions that are consent based on the survivor must be involved.

3. Revenge Porn as Gender-Based Cybercrime: Theoretical and Criminological Perspectives

To the extent that it is non-consensual intimate image abuse (NCII), or image-based sexual abuse (IBSA), the analysis of revenge porn has to be considered a paradigmatic instance of a gender-based cybercrime, which should be viewed through the perspective of feminist criminology and the overall paradigm of technology-enabled violence against women (TFVAW). Feminist criminology anticipates gender as a major power axis as well as inequality and considers such abuse not as solitary acts of deviance but as extensions of patriarchal systems of control, which attempt to exercise dominance, punish and objectify the bodies and sexuality of women. Clare McGlynn, Erika Rackley and Nicola Henry propose that IBSA creates a chain of sexual violence, where offline gender-based harms are intensified by the digital tools in creating scalable, sustained and frequently anonymous domination. This interpretation is informed by the actor-network theory and ecological theories of violence and acknowledges that technology, including social media, messaging apps, artificial intelligence, and so on, interplay with societal norms to allow abuse. In patriarchal cultures, stalkers, who are mostly men, use intimate pictures to reestablish control, retaliate alleged violations of rules like ending relationships or refusing advances, and use gendered conformity, a method designed by displaying shame in public. ITCs Frameworks on TFVAW At its foundation are frameworks on TFVAW adopted by UN Women and others that define this violence as acts perpetrated, aided or amplified by ICTs and that lead to physical, sexual, psychological, social or political or economic harm. Revenge porn can be clearly categorized as an instrument of coercion and control within this definition and as overlap between intimate partner violence (IPV) when former partners use the shared trust as a weapon to cause continued harm. Feminist criticism of the concept of revenge porn as victim-in-blame language highlights how the term suggests intentional provocation by the victim; rather, they focus on the fact that the female has been sexually subordinated by the masculine social order.

This exploitation is indissolubly connected to a network of more extensive cybercrimes that contributes to a system of related harms that cluster to make gendered vulnerability worse. Cyberstalking frequently goes hand in hand with NCII, and offenders track victims with the help of GPS positioning, social media or hacked accounts and make illusions so as to intimidate and isolate them. Digital voyeurism develops into covert videos or upskirting, and finally results in the non-consent distribution. The use of images to obtain monetary benefits, sexual compliance or silence, is considered blackmail or sextortion, particularly of women in the work position or in the public eye. Online harassment grows through doxxing personal information and photos, coordinated trolling, slut-shaming and threats of physical harassment. The overlaps form a continuum of abuse, where an initial piece of content shared initiates a domino effect of other offenses: viral content disseminated through algorithms, and perpetrators being anonymized encouraging repeat offenses. The routine activity theory of criminology focuses on motivated offenders, adequate targets (women who post images in the hope of trust) and the lack of guardians in lax platform regulation and delayed police response; feminist expansions focus on gendered opportunity structure (i.e. patriarchal norms that undermine women's digital agency) and impunity.

The damages caused are multi-layered, deep, and long-lasting, and reflect and in many cases surpass those of the direct sexual violence on the physical body. The breach of privacy undermines the bodily and informational freedom, which subjects the victims to the virtual panopticon and exposes them to continual reappearance and inability to erase the images. Sexual objectification turns women into erotic commodities consuming them, showing enhancement of the patriarchal right to leading to internalised shame. In institutional reactions, the development of secondary victimisation occurs: police victim-blaming victimisation (Why did you send it?), rejection by family, slut-shaming or disbelief of platforms, which repeats the dynamics of rape-culture that shifts the fault onto the survivors. The long-term trauma

appears in the forms of the PTSD symptoms such as post-traumatic intrusive recollections of images reappearing, hyper-vigilance to alerts or searches, avoiding intimacy, or online communication as well as anxiety, depression, suicidal ideation, loss of self-esteem, loss of trust, particularly in relations, and identity fragmentation. Economic effects are job loss, career derailment or relocation; social isolation it makes isolation worse; chronic shame brings about self-medication or withdrawal. Literature documents that victims face re-traumatisation (or continuous re-traumatisation each time they get a post or see something, their violation is refreshed), this produces a continuing threat environment, unlike one-off traumas; so victims require longer to heal, and are more likely to die by suicide.

It is essential that NCII be framed as virtual rape as it compares non-consensual image abuse to actual sexual violence and its focus on the violation of consent, power inequality and bodily harm onto a digital context. The term has itself been co-appropriated in the language of feminism, and supported by instances of metaverse attacks, or deepfake porn, denying the possibility of minimalisation (e.g. mere privacy invasion or mere porn), and pointing to experiential similarities, such as invisible lossness of bodily integrity, betrayal trauma, fear of constant violation and social disbelief. Similarly that rape abuses sexuality in order to dominate someone, NCII also violates the ability of sexual freedom by exposing someone without obtaining consent, causing the same psychological harms; powerlessness, humiliation, objectification and endlessly relying on the permanence and reach of technology to compound horror. This analogy confronts legal and cultural under-selling of digital harms, the concept of digital harms should be treated as sexual offence instead of property or privacy crime. It requires the presence of consent-focused answers, survivor-focused intervention and reforms making IBSA be treated as gendered violence that should be just regarded similarly, with prosecutive actions, deterrence, and cultural transformation breaking patriarchal cyber conventions. Representing it in this way brings together offline and online violence, and calls out the need to have the holistic criminological interventions to destroy the systemic enforcers.

One example of the gender-based aspects of cybercrime with patriarchal power structure is revenge porn, which involves the non-consent release of intimate pictures or videos to embarrass or cause harm. Theoretically speaking, feminist criminology understands it as a neo-expression of structural gender violence, in which the perpetrators of the offense are predominantly men, and use digital tools to objectify women to reinforce heteronormative power relations and homosocial masculine relationships. This parallels the transnational feminist readings of revenge porn as a transnational trespass that commodifies the bodies of women by combining online production with global hosting and offline psychological trauma and in other cases, masking the story of self-victimisation of abusers in the context of infidelity or domination within a relationship.

As a crime, it goes beyond revenge motives and includes cyber-extortion, status-making or domination, and disproportionately targets women, and the LGBTQ+ population by violating their privacy, similar to a virtual rape. The intersectional lenses expose multiple harms beginning to accumulate in the hands of marginalised groups, including women of colour who, despite not facing upper-tier harassment, experience higher rates of harassment than other online personas; empirical evidence has documented that female online personalities are subjected to disproportionately more malicious content. Their effects are tremendous emotional distress, economic loss and social stigma, which discourage reporting because of victim-blaming and inadequate legal reaction. In theory, it disrupts traditional cybercrime frameworks that only have to adopt gender-specific approaches requiring a feminist taxonomies of epistemology to the tripartite taxonomies of cybercrime (instrumental, embedded and expressive norms) to consider the other motivations except individual pathology. Deterrence needs a multi-stakeholder intervention, tech-platform responsibility and transnational laws and cultural changes on misogyny, as it contributes to the normalisation of further forms of technology-mediated gender-based violence (TFGBV). Cases are

increasing in India and a reform of the laws on cyber is much needed so as to make NCII a criminal offence to align the rights of privacy with the rights of gender justice.

4. Existing Indian Legal Framework: Key Provisions and Their Application

The country of India does not have a specific law on revenge porn and the regulations sector resorts to the Information Technology Act, 2000 (IT act), the Indian penal code as 1860 (IPC) and other complementary acts to offer justice. Some of the main provisions of IT Act include Section 66E that offends the criminalization of non-consensual interception, distribution or broadcasting of pictures of the privates and fines of 3 year imprisonment and fine of 2 lakh rupees, aiding the statutory regards to privacy. Section 67 outlaws the electronic transmission of obscene content, the violation of which is punishable by the imprisonment of three years plus a fine of 0.50 lakh INR (0.50 lakhs on a second or subsequent time), with Section 67 A seeking a punishment of five years plus the fine of 10 lakh INR (10 lakhs on a second or subsequent violation). These subsections are also applicable in the cases when the images were initially distributed on a consentual basis and further released without permission.

These provisions are reinforced by the IPC: Section 354C criminalises voyeurism, where secret filming of intimate acts should result in one to three years imprisonment, Section 354A deals with the outering of pornographic material as an offense of harassment, punishable by up to 3 years of rigorous imprisonment and Section 509 and 500 deal with insults to modesty, which shall attract penalties of up to 1 year of rigorous imprisonment. Under section 292, a two-year imprisonment sentence and a fine of up to 292 is imposed on the distribution of obscene documents (laws 292(a) and 292(b)). In the case of child victims, Section 67B of the IT Act cases punishments to a maximum of five-year imprisonment and fines worth 10 lakh rupees.

Information Technology Act, 2000 (as amended): Sections 66E (violation of privacy), 67 (obscene material), 67A (sexually explicit content), and related intermediary rules

The case applications in courts are murder City of West Bengal v. Animesh Boxi (2018), where the defendant was convicted of uploading videos of a former partner after a breakup had taken place led to a sentence of five years of rigorous imprisonment under the IPC Sections 354A, 354C, 354D, 509 and under the IT Act Sections 66E, 67, and 67A. Such behaviour has also been described by courts as similar to so-called virtual rape, invoking the right to privacy in Article 21 and ordering removal of content. However, there are still loopholes in their enforcement, which hinder early victim protection.

The main digitisation-based statutory framework relating to the dread of revenge porn or non-consensual intimate image assault (NCII) in India is the amended Information Technology Act, 2000 (IT Act), which became law in 2008. Section 66E expressly outlaws the capture, publication or transmission of an image with the intent to depict a private part of a person, their genitals, pubic region, buttocks or female breast, uncovered or merely covered by a piece of underwear, in a situation where the individual would reasonably expect privacy. The provided duty includes a term up to three years imprisonment and a fine of 200,000 rupees. This exception is especially applicable to situations of covert tape recordings or otherwise illegal sharing of intimate imagery as it is concerned with a violation of privacy, and not simple obscenity. In cases where the violators invaded devices or sent personal photographs and videos, courts have effectively invoked Section 66E. According to section 67, the act of publishing or relaying obscene information electronically is subject to a maximum sentence of three years (or five years where subsequent conviction) of imprisonment or a fine of up to 35,000 rupees (5,00,000 rupees where a second time, etc.).

Indian Penal Code/Bharatiya Nyaya Sanhita provisions: Sections 354A–354D (sexual harassment, voyeurism, stalking), 509 (insult to modesty), and others

To supplement the above laws are the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended). Under rule 3(2)(b) of the regulations, significant social

media intermediaries must take down or block access to NCII content such as nudity, exposure of body parts, sex acts, or morphing images, within 24 hours after being presented a complaint by the aggrieved party. Social media should develop complaint systems and use robotic monitoring. Failure to comply will lead to the loss of safe-harbour section 79. This framework is also consolidated in the 2025 MeitY Standard Operating Procedure, requiring 24-hour removal of NCII and deepfakes, but requiring traceability obligations on encrypted platforms in the event of grave incidents. Practically, victims are making complaints via the platform portals or cyber cells when such translates to the blocking of the URL and content removal. However, the enforcement, as with all space, is subject to immediate reporting and cooperation by the platforms as viral content and archive means normally complicate the process of permanent removal. These technological provisions supplement the legal toolset but its use is often in conflict with penal laws to offer an all-encompassing redress.

The gender-specific crimes that are codified in the Bharatiya Nyaya Sanhita, 2023 (BNS) which will replace the Indian Penal Code until July 2024 will offer significant additional provisions to the revenge porn cases. Section 75 (equivalent to the previous IPC 354A) makes sexual harassment, such as unwelcome physical advances, sexually coloured remarks, or demands to give sexual favours, criminal, and has a maximum sentence of three years imprisonment and a fine. Offenders who generate image-sharing in addition to threats or obscene remarks are consistently prosecuted under this clause.

The analogue of old IPC 509, which is now section 79, punishes the intent to humiliate the standards of decency of a woman, which is frequently applied to post an image with a degrading caption or to dox her. Other provisions concerning blackmail threats, including, but not limited to, Section 351 criminal intimidation, and general sections that pertain to defamation or hurt are cognisable and often non-bailable, allowing immediate arrests. Police normally appeal to several sections combined with the provisions of IT Act so that they would give stratified charges. The gender-specific framing acknowledges the patriarchal setting of such abuse, but critics reflect weaknesses: voyeurism is still limited to the definition of a private act that could and might not involve fully-clothed intimate images and distribution by a third party can still be avoided by direct liability. Operational wise, digital forensics (IP tracing and device recovery) is joined with victim statements by investigative officers. Convictions often come with compound sentences and as in the early cases. In general, BNS services provide a solid penal framework, highlighting sexualised harm and dignity to the victims; however, its effectiveness depends on the police training courses and the expedited procedures aimed at reducing lasting digital trauma.

Intersection with POSCO Act (for minors) and emerging data protection laws (DPDP Act, 2023)

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a civil-regulatory overlap overlaying with criminal remedies. The Act defines personal data to include intimate images as well as platforms, and making platform a data fiduciary imposing responsibilities of consent, purpose constraint, and safety of data (Sections devices 58). Victims can use the right to erasure (Section 12) and redress a grievance. Important data fiduciaries are required to have Data Protection Officers and are required to undertake data-impact assessment. Deterring smokescreens by notification and sanctions of up to 250 crores in case of non-assent. However, the DPDP is not called on criminal prosecution but on preventive compliance; it empowers the victims to petition the Data protection board to issue orders whereby the intermediaries will be ordered to delete the content permanently. Practically, the victims simultaneously use DPDP rights with a complaint to criminal authorities to seek comprehensive relief, that is, takedown through intermediaries and compensation. The consent-based approach of the Act augments the based in NCII cases as it highlights the withdrawal of consent after a relationship. The implementation issues are not eliminable because the rules are still being fully informed and the extraterritorial enforcement to foreign platforms is still unclear. Collectively, POCSO offers strong criminal penalties of child victims, whereas

DPDP presents data-rights correction of adults, thus, establishing a multilayered structure, incorporating both punitive and restorative justice in the digital ecosystem.

5. Critical Evaluation of the Adequacy of Current Laws in Addressing Revenge Porn

This critical analysis of the current legal framework in India suggests that the current situation is both a heterogeneous one concerning tackling non-consent-based intimate image abuse (NCII), herein referred to as revenge porn or image-based sexual abuse (IBSA), which is a developing form of gender-related cybercrime. Although the framework includes salient strengths, the endemic inadequacies, failures in implementation, and the relative deficits all indicate its ineffectiveness in the current digital environment, especially in the face of mounting artificial-intelligence-oriented issues, such as deepfakes.

Key strengths of the regime can be traced in the fact that the gender-neutral provisions of the Information Technology Act, 2000 (IT Act) are applicable to all types of victims irrespective of their gender; hence, it becomes possible to prosecute in a variety of situations. Section 66E directly addresses infractions of privacy occurring by way of intercepting and sending of images of the private area without consent, where the Sections 67 and 67A criminalise the production and publicizing of obscene and sexually explicit electronic contents, and thus covers downstream sharing. This punitive system is based on deterring, prescriptive penalties of up to seven years and fines of up to ₹101akh, and often augmented by the Bharatiya Nyaya Sanhita (BNS) penalties, including section 77 about voyeurism, in order to effect cumulative punishment. Courts have gone around piecemeal statutes by inventive judicial restraint, with the most notable decisions over the years including victims as rape victims with protection against wrongful injury, that notwithstanding the 'right to be forgotten' will include compulsory delinking, and most recently promulgation of a standard operating procedure to effect an instantaneous takedown. Intermediary rules and 2025 ministry of electronics and information technology (MeitY) NCII SOP place a duty of timely action on platforms thus making preventive enforcement more effective. All these aspects are indicative of flexibility, as seen in high-profile criminal cases and a proven willingness to protect digital dignity.

However, the holes in the legal framework are significant, and its flaws also contribute to a stronger effect. This absence of a specific, independent law on NCII, or revenge porn, makes the regime mottled and partial and thus requires the system to fall back on privacy, obscenity, or voyeurism laws that refacilitates the problem into a question of indecency over a failure to honor consent and a gendered expression of sexual violence. Limiting statutory definitions restrict the scope of the protection: e.g., the provision of voyeurism in section 77 of the BNS (previously IPC section 354C) is mostly focused on the original capturing of images in private, making it in most cases irrelevant to later third-party sharing, changes that are not advertently revealing a private part or to images which are clothing-covered and of sexual implication. Notably, the legal texts lack a consent-based structure; they do not specifically criminalise the denial, withdrawal and revocation of the consent and they do not regulate the threat to spread NCII, the production of a synthetic (deepfake) piece of content without an original source image or even possession to distribute it. As a result, professionals can avoid responsibility regarding AI-based NCII or non-explicit but humiliating share. The civil remedy provided by the Data Protection and digital privacy Law (DPDPL) of 2023 includes erasure but does not include any criminal liability when risks in the forms of gendered harms occur. Furthermore, the rules in the middle assume complaints initiated by the victim in place of proactive regulation and the legal regime is ill-set to address the distinct irreversibility, extensibility and psychological parity of IBSA and corporeal sexual offence, and, as a result, the legal regime continues to victimise the victim.

The constitutional shortcomings are also aggravated by practical implementation, which makes statutory clauses ineffective. Evidential barriers remain: intent establisement, understanding anonymous uploads across applications, integrity of digital artefacts, especially in encrypted systems, and authenticating deepfakes present an overall burden on under-manned cyber departments. It is still cultural victim-blaming, the police tend to dismiss any complaints by saying why share the photo, why file an FIR, or

shift the attention to what might be wrong or wrong with the alleged behaviour of the victim, which is a deterrent to reporting in the face of stigma. They still permeate delays in content action: despite the 24 hour removal requirement embodied in the IT rules and the SOP that goes into effect in 2025, viral distribution, reposting, and foreign inaction make permanence impossible, and further prolongs the trauma. The process of sensitising the police is incomplete; a large portion of the police are not trained in digital forensics, gender-sensitive protocols, or choosing protocols that are survivor-oriented, which results in mis-handled cases. Conviction rates are alarmingly low: the data of the National Crime Records Bureau and independent studies show that cybercrime perpetrated against women is tried successfully in less than 20% of cases, and that the case against cybercrime perpetrated by a woman is acquitted in most cases because of the lack of evidence, loss of the testimony of a victim following a long process in the court, and the long queues in the court. Cases of low reporting, which are not adequately reflected in the statistical aggregates as well as cultural barriers also reduce the deterrent effect.

6. Emerging Challenges in the Digital Age: Deepfakes, AI, and Future-Proofing Protections

The cross-jurisdictional analysis highlights India as underdeveloped and provides directions of reform. The United Kingdom has just passed some progressive legislation, which is the amendment to the Sexual Offences Act (after 2024) making the distribution or threat of distribution of intimate images a criminal offense that does not require demonstration of intent to cause distress, providing deepfakes content as expressly included, and a five-year prison sentence as a sentencing range. It requires platforms to inhibit 48-hour takedown court orders under the Online Safety Act and to designate priority-offending material status to child sexual abuse material as well, and deploy hashing-based assurance instruments, including StopNCII.org, with greater reporting outcomes and takedown success. The anti-Photo and video voyeurism law of the Philippines, the law that stipulates a penalty of five years, should one capture or share pictures without proper authorization (Anti-photo / video voyeurism act, 2009, RA 9995), and a 24-48-hour removal requirement is proposed by the anti-deep-fake legislation under the brand name Take It Down Act (anti-deep-fake -1, 2022). The actions of the European Union bearing fruit in two items: Directive 2024/1385 criminalizing non-consensual sharing, cyberstalking, and incitement; article Digital Services Act places an immediate responsibility on platforms and survivorship protection. similar thematic elements are found in these jurisdictions: consent-based, autonomous crimes, proactive platform liability, civil relief approaches and specialised investigation units- another world to the reactive, disjointed Indian model. The following recommendations are derived: need to promulgate specific NCII laws; specific consent-based definitions; hashing and takedown must be mandatory; police should be trained; and fast-track courts.

In short, even though the present legal framework in India provides the conceptual tools and shows judicial creativity, its disjointed statutory nature, limited jurisdiction, and weak enforcement structures are unsuitable when it comes to addressing the dynamic landscape of gendered digital violence. The comparative jurisprudence highlights a need to enact legislative changes that are reforms made alone and are based on consent so that strong protection may be guaranteed in the hyper-digital India society.

7. Conclusions and Recommendations: Towards Comprehensive Reform

Although India has a framework that offers punitive devices, it does not offer prevention strategies, swift redress, and acknowledgment of the unanimous feminized, technology enabled violence by NCII. Embarking on wholesale reform is thus urgent: the creation of non-consensual intimate image abuse standalone legislation; amendment of the IT Act to pre-empt consent and non-bailable status; improvement of the intermediary liability; the adoption of victim support services through legislation; and the propagation of public awareness efforts; and enhancement of intermediary accountability. These would be more effective to protect the digital integrity of women, and punish those who commit such crimes and bring laws closer to the realities of the hyper-interconnected Indian society hence justice in the digital era with the need to limit freedom of expression.

References

[1] Halder, A., & Basu, D. (2025). Digital privacy at risk: Examining India's legal response to non-consensual sharing of intimate media. International Journal of Law and Social Sciences, 4(2), 45–67.

[2] https://ijlsss.com/digital-privacy-at-risk-examining-indias-legal-response-to-the-non-consensual-sharing-of-intimate-media/

[3] Kavitha, T. (2025). Revenge porn and image-based sexual abuse in India: Victimisation, legal responses, and emerging challenges. Indian Journal of Law and Legal Research, 6(4), 112–130.

[4] https://www.ijllr.com/post/revenge-porn-and-image-based-sexual-abuse-in-india-victimisation-legal-responses-and-emerging-cha

[5] Sharma, R. (2025). Legal gaps in addressing revenge porn and deepfake pornography in India. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 8(1), 20–35.

[6] https://ijmrset.com/upload/44_Legal%20Gaps%20in%20Addressing%20Revenge%20Porn%20and%20Deepfake%20Pornography%20in%20India.pdf

[7] Yadav, S. (2024). Legal and policy context of revenge pornography: A study of Indian cases. UPES Doctoral Repository.

[8] https://dr.ddn.upes.ac.in/bitstream/123456789/4439/1/Shilpi%20Yadav%20Phd%20Thesis.pdf

[9] Singh, A. (2025). Public awareness and legal reforms for combating revenge porn. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 8(3), 78–92.

[10] https://www.ijmrset.com/upload/61_Public%20Awareness%20and%20Legal%20Reforms%20for%20Combating%20Revenge%20Porn.pdf

[11] India Law Offices. (2024). Revenge porn or non-consensual pornography. India Law Offices Legal Articles.

[12] https://www.indialawoffices.com/legal-articles/revenge-porn-or-non-consensual-pornography

[13] Gupta, N. (2025). Protecting women's privacy: Evolving cyber laws against harassment in India. Law Curb Journal, 2(1), 15–28.

[14] https://www.lawcurb.in/post/protecting-women-s-privacy-evolving-cyber-laws-against-harassment-in-india

[15] Rao, V. (2025). Revenge porn and deepfake: Is India ready for AI-borne sexual exploitation? Into Legal World, 3(4), 50–65.

[16] https://www.intolegalworld.com/post/revenge-porn-and-deepfake-is-india-ready-for-ai-borne-sexual-exploitation

[17] Patel, M. (2022). Inadequacy of laws dealing with revenge porn in India. Indian Journal of Law and Legal Research, 3(2), 237–250.

[18] https://doi-ds.org/doilink/01.2022-17589277/IJLLR/V3/I2/A237

[19] Kumar, R. (2025). Legal implications of deepfake technology in India. Indian Journal of Law Review, 5(9), 6–22.

[20] https://ijlr.iledu.in/wp-content/uploads/2025/06/V5I96.pdf

[21] Anonymous. (2024). Legal provisions related to non-consensual sharing of intimate images: A comparative analysis. International Institute of Research in Cyber Justice. https://iircj.org/wp-content/uploads/92.Legal-Provisions-Related-to-Non-Consensual-Sharing-of-Intimate-Images-A-Comparative-Anal ...

[22] IT for Change. (2023). Justice in the digital age: Addressing non-consensual dissemination of intimate images in India's penal code. P39A Blog. https://p39ablog.com/2023/05/justice-in-the-digital-age-addressing-non-consensual-dissemination-of-intimate-images-in-indias-pen