REVENGE PORN AND IMAGE-BASED SEXUAL ABUSE IN INDIA: VICTIMISATION, LEGAL RESPONSES, AND EMERGING CHALLENGES

Kavitha T, The Tamil Nadu Dr. Ambedkar Law University

ABSTRACT

This article explores the escalating issue of revenge pornography and image-based sexual abuse (IBSA) in India from both victimological and legal perspectives. It assesses the psychological effects of IBSA on victims, emphasizing the persistent, borderless, and lasting nature of digital harm. The paper provides a critical analysis of India's current legal framework under the Information Technology Act and the Indian Penal Code, pinpointing deficiencies in enforcement, evidentiary hurdles, and institutional insensitivity. Comparative analyses from jurisdictions such as the United Kingdom, Australia, the United States, Canada, and New Zealand demonstrate the efficacy of specialized IBSA legislation, national regulatory agencies, and civil remedies. Drawing lessons from these examples, the article recommends essential reforms, including the establishment of a standalone IBSA law, enhanced intermediary liability, trauma-informed policing practices, improved digital forensic capabilities, and comprehensive public awareness initiatives. In summary, the study highlights the necessity for a coherent, survivor-focused, and technologically adaptive strategy to effectively combat IBSA in India.

Keywords: Sexual Abuse, digital harm, trauma, Survivor-focused.

1. INTRODUCTION:

Digital technology has significantly altered interpersonal relationships, communication methods, and the characteristics of modern crime. The widespread availability of smartphones, fast internet connectivity, encrypted messaging applications, and social media platforms has allowed individuals to share personal and intimate content with an unprecedented level of convenience. Nevertheless, this integration of technology has given rise to detrimental behaviours that exploit intimacy. Among these is revenge porn defined as the non-consensual sharing of intimate images, frequently occurring after conflicts in relationships which has become a notable danger. This issue falls under the larger umbrella of image-based sexual abuse (IBSA), which includes actions such as non-consensual recording, threats to distribute images, voyeurism, deepfake pornography, and extortion involving intimate visual content.

In India, the socio-cultural context in which sexuality is perceived and governed intensifies the damage inflicted by such offenses. The public dissemination of private images frequently leads to moralistic condemnation, damage to reputation, familial ostracism, and in certain instances, physical aggression. As a result, Image-Based Sexual Abuse (IBSA) signifies not merely a technological offense but also a social and psychological trauma rooted in deep-seated gender inequalities and patriarchal standards. Although the Indian legal framework offers various statutory provisions pertinent to these offenses, it remains disjointed and insufficient in light of the rapid evolution, extensive reach, and intricate nature of digital technologies. This essay seeks to deliver a scholarly, thorough examination of revenge porn and IBSA in India through conceptual analysis, victimological insights, and legal assessment.

2. Conceptual Framework: Understanding Revenge Porn and Image-Based Sexual Abuse

2.1 Defining Revenge Porn:

“Revenge porn” generally refers to the non-consensual sharing of sexually explicit images or videos online by a current or former intimate partner, often with the intent to shame, harass, or exact revenge on the victim.[1]

However, scholars argue that the term is misleading because it implies that the offender’s

[1] Clare McGlynn & Erika Rackley, Image-Based Sexual Abuse, 37 Oxford J. Legal Stud. 534 (2017).

motive is always retaliation and that the victim did something to deserve "revenge." Consequently, contemporary criminology and feminist literature prefer the broader term Image-Based Sexual Abuse (IBSA).

2.2 Based Sexual Abuse (IBSA) as a Broader Category:

IBSA encompasses the following actions:

1. The non-consensual acquisition of intimate images (for instance, through hidden cameras).
2. The non-consensual distribution or dissemination of intimate images.
3. Threats to distribute intimate images as a means of coercion or extortion.
4. Sexualized deepfakes (images that have been digitally manipulated or AI-generated pornography).
5. The morphing of photographs, which includes the digital alteration of innocent images for sexual purposes.
6. Voyeurism, which involves recording individuals without their consent.
7. The storage, reproduction, or circulation of intimate images without the consent of the individuals depicted.

Academics categorize IBSA as a type of sexual violence and technology-facilitated gender-based violence, highlighting the harmful intent to undermine dignity, autonomy, and privacy.[2]

2.3 Victim–Offender Relationship:

Research indicates that in the majority of IBSA incidents, the perpetrator is:

1. An ex-partner,
2. A present intimate partner,

[2] Nicola Henry & Anastasia Powell, Technology-Facilitated Sexual Violence: A Literature Review, 19 Violence Against Women 113 (2013).

3. A friend or acquaintance, or

4. stranger taking advantage of stolen information.

This occurrence is fundamentally entrenched in gendered power dynamics, coercive control, and the male sense of entitlement regarding women's bodies.

3. Evolution of Revenge Porn and IBSA in the Digital Context:

- **Technological and Social Driver.**

a. Smartphone Proliferation: The swift availability of high-definition cameras has led to an increase in the production and preservation of personal media.

b. Cloud Storage & Social Media Platforms: These platforms facilitate the rapid widespread sharing of content with minimal accountability.

c. Anonymity on the Internet: Perpetrators are encouraged by the reduced likelihood of being caught due to the low immediate risks associated with detection.

d. Patriarchal Social Structures: Women encounter heightened stigma and shame, rendering them more vulnerable to such offenses

- **From Private Harassment to Public Degradation:**

Historically, intimate partner violence was largely limited to physical or emotional realms. However, the advent of technology has expanded this violence into the digital realm, rendering it permanent, without borders, and difficult to manage. Cybercrimes that involve intimate images inflict lasting damage, as once such content is disseminated, it can be:

a. Downloaded,

b. Redistributed,

c. Stored on external servers,

d. Shared on adult content forums.

Consequently, Image-Based Sexual Abuse (IBSA) has developed into one of the most severe forms of digital victimization.

4. Victimisation and Psychological Impact:

Victimisation in instances of revenge porn and image-based sexual abuse (IBSA) is complex, impacting the psychological, social, emotional, and behavioural aspects of the victim's existence. Unlike conventional forms of sexual victimisation, IBSA is particularly devastating due to the ongoing, borderless, and uncontrollable nature of the harm once intimate images are shared in digital environments. Victims frequently feel an overwhelming sense of powerlessness, as the permanence and replicability of online content foster the belief that the abuse will never truly cease. This situation transforms digital victimisation into a chronic trauma rather than a singular event.[3]

From a psychological perspective, victims often report experiencing depression, severe anxiety, panic attacks, and symptoms akin to post-traumatic stress disorder (PTSD). The anxiety that intimate images could resurface at any moment results in hypervigilance, sleep disruptions, and ongoing stress. Victims may mentally replay the incident, suffer from intrusive thoughts, and constantly monitor online platforms, leading to a cycle of emotional fatigue. In numerous instances, victims internalise feelings of shame, guilt, and self-blame emotions that are exacerbated by societal attitudes that unjustly scrutinise the victim's morality or decisions.[4]

Socially, the stigma associated with sexual imagery amplifies psychological damage. In conservative cultures such as India, where honour and modesty are intricately linked to female sexuality, victims particularly women often endure secondary victimisation from family, peers, law enforcement, and the broader community. This additional harm can frequently surpass the initial trauma, resulting in social withdrawal, isolation, and the erosion of support networks. Victims may shun public spaces, halt their education, or leave their jobs due to the fear of humiliation or harassment.[5]

[3] Nicola Henry & Anastasia Powell, Technology-Facilitated Sexual Violence: A Literature Review, 19 Violence Against Women 113, 120 (2013).
[4] Amanda Lenhart et al., Non-Consensual Image Sharing: Psychological Effects, Pew Research Centre Report (2016).
[5] William G. Doerner & Steven P. Lab, Victimology 178 (7th ed. 2015).

5. Legal Responses in India:

Legal responses to revenge porn and image-based sexual abuse (IBSA) in India are dispersed across various statutes instead of being unified under a single, comprehensive law. Although there is no specific "Revenge Porn Act," Indian legal frameworks, including the Information Technology Act, 2000 (IT Act), the Indian Penal Code, 1860 (IPC) / Bharatiya Nyaya Sanhita (2023), and specialized laws such as the Protection of Children from Sexual Offences Act, 2012 (POCSO), collectively tackle multiple aspects of IBSA. Nonetheless, the fragmented nature of these regulations frequently results in difficulties regarding prosecution and enforcement.

A. Information Technology Act, 2000:

The IT Act is pivotal in overseeing online sexual content.

- **Section 66E**, which addresses privacy violations, criminalizes the intentional capturing, publishing, or transmitting of images depicting private parts without consent. This section is directly relevant to instances where intimate images are shared online. Section 67 imposes penalties for the publication or transmission of obscene material in electronic formats.[6]

- **Section 67A** specifically targets the dissemination of sexually explicit content; this provision is often applied in cases of revenge porn. In situations involving minors,[7] **Section 67B** pertains to child sexual abuse material, encompassing the storage, transmission, or creation of sexual content that involves children.[8]

Although the IT Act holds technological significance, its dependence on the term "obscenity" a term criticized for its ambiguity restricts its capacity to adequately address the complex harm associated with the non-consensual sharing of intimate images. Furthermore, the Act fails to explicitly acknowledge IBSA as a separate category of sexual violence.

B. India Penal Code,1860:

Several sections of the IPC complement the IT Act. **Section 354C (BNS-Sec 77)**, which was

[6] Information Technology Act, No. 21 of 2000, § 66E (India).
[7] Id. §§ 67–67A.
[8] Id. § 67B.

introduced by the Criminal Law (Amendment) Act of 2013, makes voyeurism a criminal offense and specifically addresses the act of taking or sharing images of women engaged in private activities without their consent.[9]

- **Sections 354A (BNS-Sec 74) and 354D (BNS-Sec 78),** which relate to sexual harassment and stalking, are applicable when intimate images are utilized to harass, coerce, or blackmail victims.

- **Section 499 (BNS-Sec 356)**, which provides a definition of defamation, along with **Section 509 (BNS-Sec 79)**, which imposes penalties for insulting a woman's modesty, can be invoked when the distribution of images is aimed at degrading or shaming the victim.[10]

- Offenses that involve threats to publish intimate content are governed by **Sections 503 (BNS – Sec 351) and 506 (BNS-Sec 351)**, which address criminal intimidation.[11] Nevertheless, the provisions of the IPC are constrained by gender-specific language many sections offer protection solely to female victims resulting in insufficient coverage for male and LGBTQ+ victims.

C. POCSO Act, 2012:

The POCSO Act provides robust protections for minors. It makes it a criminal offense to record, distribute, or possess sexual images of children under **Sections 13–15**, acknowledging child pornography as a grave crime. In light of the increasing prevalence of teenage sexting and digital grooming, POCSO has become essential for prosecuting cases that involve minors.

D. Judicial Responses:

The Indian judiciary has progressively recognized the serious implications of IBSA. In the case of **X v. State of Karnataka**, the Karnataka High Court noted that the non-consensual sharing of intimate images infringes upon the constitutional rights to dignity and privacy as outlined in Article 21[12]. Similarly, in **State of West Bengal v. Animesh Boxi**, the Calcutta High Court

[9] Indian Penal Code, No. 45 of 1860, § 354C (India).
[10] Id. §§ 499, 509.
[11] Id. §§ 503–506.
[12] X v. State of Karnataka, 2022 SCC Online Kar 554.

found the defendant guilty of posting altered intimate photographs, acknowledging these actions as forms of sexual exploitation and psychological harm.[13] Furthermore, courts have mandated the rapid removal of such content from online platforms, highlighting the necessity for immediate corrective measures.

E. Institutional and Procedural Mechanisms:

India has set up Cyber Crime Cells, the National Cyber Crime Reporting Portal, and specialized police units to facilitate the reporting process. Victims have the option to request takedown orders, and proceedings are frequently held in-camera to safeguard privacy. Nevertheless, the lack of cyber-forensic expertise, societal stigma, and varying responses from intermediaries hinder effective enforcement.

F. Need for a Consolidated Framework:

In spite of various provisions, the lack of a specific IBSA statute leads to uncertainty. A unified legal framework that acknowledges IBSA as a unique type of sexual violence utilizing gender-neutral terminology, prompt removal procedures, accountability for platforms, and processes focused on victims is crucial for effective protection.

6. Reporting Mechanisms and Victim Assistance in India

The emergence of revenge pornography and image-based sexual abuse (IBSA) in India has revealed significant structural deficiencies in the processes for victim reporting and the provision of substantial assistance. Victims mainly women and minors frequently face challenges stemming from fear, shame, social stigma, and institutional obstacles when attempting to seek help, leading to considerable under-reporting. Consequently, an effective response from the justice system necessitates not only strong legal frameworks but also easily accessible reporting mechanisms and support systems that are informed by an understanding of trauma.

Online Reporting Platforms:

The Government of India has set up the National Cyber Crime Reporting Portal (NCCRP) to

[13] State of West Bengal v. Animesh Boxi, 2018 SCC Online Cal 4866.

enable victim-friendly reporting of cybercrimes, including sexual exploitation.[14] This portal permits anonymous complaints, which is particularly important for victims who are reluctant to reveal their identity due to fears of retaliation or societal judgment. This feature is instrumental in addressing the prevalent hesitation among survivors of Image-Based Sexual Abuse (IBSA) to approach conventional police stations. Furthermore, the portal collaborates with various state cyber cells, ensuring that complaints are routed to the correct jurisdiction.

In addition to the NCCRP, victims have the option to report content directly on social media platforms, which are required under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to remove non-consensual intimate images within a specified timeframe. Intermediaries such as Facebook, Instagram, and X (formerly Twitter) provide built-in reporting mechanisms for content related to sexual exploitation.[15] Nevertheless, adherence to these guidelines is inconsistent, and delays in content removal often exacerbate harm and distress.

Police Reporting and Investigative Support:

Victims may also lodge a First Information Report (FIR) at any police station, regardless of jurisdiction, under the "Zero FIR" mechanism.[16] This provision is particularly important in cases where the victim may be too distressed to travel or may be subjected to intimidation by local actors. Several states operate dedicated cyber police stations and cyber helpdesks in district-level units, which are equipped with trained personnel and digital forensic tools.

However, challenges persist. Studies indicate that police officers often lack training on gender-sensitive investigation, data preservation, and digital evidence collection, resulting in re-victimisation.[17] Survivors frequently report moralistic attitudes during police interviews, particularly in conservative regions, which deters further reporting.

Victim Assistance and Support Services:

Victim assistance in India functions through a blend of governmental and civil-society frameworks. The One-Stop Centres (OSCs) established by the Ministry of Women and Child

[14] National Cyber Crime Reporting Portal, Ministry of Home Affairs, Govt. of India.
[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[16] Lalita Kumari v. Govt. of Uttar Pradesh, (2014) 2 SCC 1.
[17] Pratiksha Baxi, Rape Cultures in India, 23 Gender & Soc'y 25 (2019).

Development offer emergency medical services, psycho-social support, legal aid, and temporary accommodation.[18]

While primarily aimed at addressing physical crimes against women, numerous OSCs have broadened their support to include survivors of cyber-enabled sexual violence.

Non-governmental organizations such as the Cyber Peace Foundation, Centre for Social Research, and India provide training on digital safety, assist with takedown requests, guide victims through the cyber police processes, and deliver counselling services. These organizations are vital in connecting victims with state institutions.[19]

The Victim Compensation Schemes outlined in **Section 357A (BNSS-Sec 396)** of the Code of Criminal Procedure provide financial compensation for trauma, legal expenses, and rehabilitation. Some states have specifically incorporated victims of cyber sexual harassment into their compensation frameworks. However, the application process is often bureaucratic, and victims frequently lack the legal support necessary to access these benefits.[20]

Toward a Victim-Centric Approach:

In spite of structural advancements, India still does not possess a fully victim-centred framework for tackling IBSA. Obstacles such as societal stigma, insufficient digital literacy, inadequate law enforcement capabilities, and slow platform compliance continue to weigh heavily on survivors. Looking ahead, reforms should focus on:

- Comprehensive training for law enforcement in digital forensics and trauma-informed interviewing;
- Efficient multi-agency collaboration for swift takedown actions; and
- The growth of counselling and legal aid networks based on victimology principles. It is crucial to ensure that survivors receive timely, respectful, and comprehensive support to mitigate the enduring psychological and social damages caused by revenge porn and image-based abuse.

[18] Ministry of Women and Child Development, One Stop Centre Scheme (2015).
[19] Cyber Peace Foundation, Annual Report on Cyber Safety Initiatives (2023).
[20] Code of Criminal Procedure, 1973, § 357A.

7. Challenges in Legal and Practical Implementation:

Despite the presence of legal provisions under the Information Technology Act, 2000 and the Indian Penal Code, India's approach to revenge pornography and image-based sexual abuse (IBSA) continues to encounter significant legal and practical obstacles. These deficiencies not only diminish deterrence but also intensify the trauma faced by victims. A victimological viewpoint emphasizes that the law's efficacy relies not solely on its enactment but also on its enforceability, accessibility, and sensitivity towards survivors.

1. Fragmented Legal Framework and Overlapping Provisions:

A major challenge is the fragmented character of India's legal framework, which necessitates that victims navigate through various overlapping provisions. Offences related to IBSA are dispersed across Section 66E (violation of privacy) and Sections 67, 67A, and 67B of the IT Act, in addition to IPC Sections 354C (voyeurism), 354D (stalking), and 509 (insulting modesty).[21] While these provisions collectively criminalize non-consensual imagery, the lack of a singular comprehensive statute specifically targeting IBSA results in ambiguity during investigations and prosecutions. Law enforcement officials often misinterpret technological details, resulting in improper FIR registrations or inadequate charging of offences.[22]

2. Evidentiary Complexities and Digital Forensics:

Digital crimes inherently present challenges concerning the preservation, acquisition, and admissibility of electronic evidence. Images and videos shared online can be modified, erased, or duplicated across various platforms in a matter of minutes. Although Section 65B of the Indian Evidence Act outlines procedures for certifying electronic evidence, acquiring timely certificates from service providers or platform intermediaries remains a significant challenge. Numerous police stations are equipped with inadequate digital forensic tools, outdated software, and personnel lacking the necessary training to recover deleted media or trace digital footprints. Consequently, evidence that is vital for securing convictions often becomes irretrievable or inadmissible.[23]

[21] Information Technology Act, 2000, §§ 66E, 67–67B; Indian Penal Code, 1860, §§ 354C, 354D, 509.
[22] Aparna Viswanathan, Cyber Crimes Against Women in India, 12 NLUD J. Legal Stud. 45 (2022).
[23] Indian Evidence Act, 1872, § 65B.

3. Intermediary Non-Compliance and Delayed Takedowns:

Although the IT Rules, 2021 require intermediaries to eliminate non-consensual sexual content within twenty-four hours of receiving a complaint, adherence to this mandate is inconsistent. Global platforms frequently operate via foreign servers, resulting in slow and bureaucratic communication. Victims often report delays in the removal of content, during which their images continue to be accessed, downloaded, or redistributed intensifying their trauma. Smaller platforms, pornographic websites, or anonymous forums may entirely refuse to cooperate or temporarily shut down to avoid liability.

4. Police Insensitivity and Lack of Gender-Responsive Practices:

Victims of Image-Based Sexual Abuse (IBSA) frequently face insensitive and moralistic attitudes at police stations, particularly in smaller towns and rural regions. Numerous officers downplay the severity of the offense, hold victims accountable for sharing intimate images, or dissuade them from filing First Information Reports (FIRs) to prevent "family shame." Lack of specialized training in cyber-victimization, trauma-informed interviewing, and digital evidence leads to secondary victimization, which further discourages survivors from seeking assistance. Women and minors encounter additional obstacles due to fears of societal stigma and pressure to remain silent.

5. Limited Awareness and Digital Literacy:

A significant portion of the Indian populace lacks sufficient digital literacy, hindering victims from comprehending how to report offenses, document evidence, or secure their online accounts. Awareness regarding the National Cyber Crime Reporting Portal, intermediary reporting mechanisms, or victim assistance services is notably low. This deficiency allows perpetrators to exploit vulnerabilities and dissuades victims from seeking legal recourse.[24]

6. Judicial Backlogs and Slow Prosecution:

Even when cases advance to court, judicial delays compromise the effectiveness of legal remedies. Courts face challenges with technological interpretation, cross-jurisdictional issues, and limited forensic support. Victims endure extended litigation, during which emotional

[24] Cyber Peace Foundation, Digital Awareness Survey Report (2023).

distress, reputational damage, and fear of further exposure continue to persist.

8. Comparative Approaches: Lessons for India:

As digital technologies continue to evolve and personal interactions increasingly transition to online platforms, countries globally have been urged to develop legal frameworks to tackle revenge pornography and image-based sexual abuse (IBSA). Although India has made significant progress through the IT Act, amendments to the IPC, and the 2021 Intermediary Rules, the nation still faces challenges related to enforcement gaps, complexities in evidence, and a lack of sensitivity within institutions. Analysing international models offers important insights for creating a more effective and survivor-focused approach.

1. United Kingdom: A Committed Statutory Offence and Victim-Focused Strategy

The United Kingdom is frequently referenced as an exemplary model due to its explicit criminalization of revenge pornography. According to Section 33 of the Criminal Justice and Courts Act 2015, the UK clearly forbids the distribution of private sexual images and videos without consent and with the intention of causing distress. This focused strategy provides the clarity that is absent in India's disjointed legal framework.[25]

Moreover, the UK's strategy includes protective anonymity for victims, ensuring that individuals affected by Image-Based Sexual Abuse (IBSA) are safeguarded from media exposure. Specialized police units, such as the Revenge Porn Helpline, support victims in reporting incidents, submitting takedown requests, and accessing emotional assistance. This combined framework legal precision alongside institutional backing significantly mitigates secondary victimization and empowers survivors to pursue justice.

India could benefit from the UK's model by implementing a distinct law that specifically addresses IBSA, clearly defining offenses, procedures, and penalties in a cohesive and technologically aware manner. Furthermore, instituting statutory anonymity protections could help prevent victims from retracting complaints due to fears of stigma or damage to their reputation.

[25] Criminal Justice and Courts Act 2015, c. 2, § 33 (U.K.).

2. Australia: Frameworks for Technology-Facilitated Abuse and Civil Penalties.

Australia offers another strong model through its eSafety Commissioner, an independent statutory entity with the authority to mandate the removal of non-consensual intimate images from various platforms. The Enhancing Online Safety Act 2015 grants the Commissioner the power to issue removal notices that must be acted upon within 48 hours. Non-compliance results in financial penalties imposed on platforms or offenders.[26]

In addition, several Australian states including New South Wales, Victoria, and South Australia have established comprehensive laws addressing IBSA, which encompass the creation, distribution, and threats of dissemination. These regulations acknowledge the psychological distress associated not only with the circulation of such images but also with coercive threats.

India can draw valuable lessons from this by creating a national regulatory authority that possesses technical expertise and the authority to mandate the swift removal of content by intermediaries. Although the Indian Intermediary Rules require removal within 24 hours, the enforcement of this rule is often inconsistent. A dedicated authority, equipped with investigative and forensic capabilities akin to Australia's eSafety model could effectively address this issue.

3. United States: State-Level Diversity and Civil Remedies

In the United States, laws regarding revenge porn differ from state to state, with over 48 states criminalising non-consensual pornography. Importantly, the U.S. framework combines criminal, civil, and tort-based remedies.[27] Survivors have the option to pursue injunctions, restraining orders, and compensation for emotional distress and damage to their reputation. Civil remedies often provide faster relief, particularly in instances where digital evidence does not satisfy criminal standards.

Additionally, platforms function under the Digital Millennium Copyright Act (DMCA) takedown process, which enables victims to request the removal of intimate images on copyright grounds, even if they did not upload the content themselves. This process frequently acts as an effective non-criminal method for content removal.

[26] Enhancing Online Safety Act 2015 (Austl.); Office of the eSafety Commissioner, Annual Report (2022).
[27] Cyber Civil Rights Initiative, State Revenge Porn Laws (2023).

For India, broadening civil remedies such as compensation, injunctions, and privacy-focused tort actions could enhance the existing criminal provisions. Victims who are apprehensive about criminal proceedings due to societal stigma or the trauma of cross-examination may find civil law options more beneficial, as they prioritise privacy and provide prompt interim relief.

9. Lessons for India:

A comparative analysis reveals several clear directions:

a. Enact a standalone IBSA legislation

India's scattered provisions create confusion. A comprehensive statute, similar to the UK or Australian model, could provide clarity, consistency, and enhanced victim protection.

b. Establish a national digital safety authority

A centralised, well-equipped body could ensure rapid content takedowns, oversee platform compliance, and support victims.

c. Strengthen civil remedies and privacy torts

Drawing from U.S. and Canadian practices, providing compensation, injunctions, and restorative options would offer holistic redress.

d. Provide anonymity and victim-friendly procedures

Statutory anonymity, trauma-informed policing, and specialised victim support units would reduce secondary victimisation.

e. Promote digital literacy and awareness

International experience shows that legal measures alone are insufficient; public education campaigns are essential for reducing vulnerability and encouraging reporting.

10. Conclusion:

Suggestions and Recommendations:

Addressing the issues of revenge pornography and image-based sexual abuse (IBSA) in India

necessitates a coordinated, survivor-focused, and technology-informed strategy. To begin with, India should contemplate the enactment of a comprehensive standalone law on IBSA that explicitly defines non-consensual intimate imagery, criminalizes the distribution and threats of dissemination, and establishes uniform procedures for investigation and victim protection. A consolidated statute would eliminate the ambiguity created by the scattered provisions found in the IPC and IT Act. Furthermore, the creation of a National Digital Safety Authority, inspired by Australia's eSafety Commissioner, is imperative. This organization should possess the authority to issue binding takedown orders, collaborate with global intermediaries, assist victims with counselling and evidence preservation, and enhance national digital forensic capabilities. Additionally, it is essential to strengthen platform accountability by enforcing strict deadlines for content removal, imposing penalties for non-compliance, and mandating the use of proactive detection tools to prevent the re-uploading of intimate images.

Moreover, specialized training for law enforcement and the judiciary is vital to ensure trauma-informed management of complaints, accurate registration of offenses, and effective utilization of digital evidence. Lastly, ongoing public awareness and digital literacy initiatives are crucial to empower individuals to identify, report, and prevent IBSA. Collectively, these measures can foster a safer and more responsive digital environment for victims.

Reference:

1. William G. Doerner & Steven P. Lab, *Victimology* (7th ed. 2015).

2. Matthew Hall, *Victims of Crime: Policy and Practice* (2d ed. 2017).

3. Clare McGlynn & Erika Rackley, Image-Based Sexual Abuse, 37 Oxford Journal of Legal Studies 534 (2017).

4. Nicola Henry & Anastasia Powell, Technology-Facilitated Sexual Violence: A Literature Review, 19 Violence Against Women 113 (2013).

5. Pranesh Prakash, Gendered Dimensions of Cyber Harassment in India, 12 Indian Journal of Criminology 44 (2019).

6. Shawna Coxon, Revenge Porn as Sexual Violence, 24 Canadian Journal of Women & the Law 277 (2012).

7. Aparna Viswanathan, Cyber Crimes Against Women in India, 12 NLUD Journal of Legal Studies 45 (2022).

8. Amanda Lenhart et al., *Non-Consensual Image Sharing: Psychological Effects*, Pew Research Centre (2016).

9. Cyber Peace Foundation, *Digital Awareness Survey Report* (2023).

10. Information Technology Act, No. 21 of 2000, India Code §§ 66E, 67–67B.

11. Indian Penal Code, No. 45 of 1860, India Code §§ 354C, 354D, 509.

12. Indian Evidence Act, No. 1 of 1872, § 65B.

13. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, Gazette of India, 2021.