WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# SECONDARY VICTIMIZATION IN DIGITAL SEX CRIMES AND ONLINE ABUSE LITIGATION

*[1.] Akashdeep Kour [2.] Mr. Nikhil Jain*

**[1] Email id- kourakashdeep6@gmail.com**
**LL.M. Student Jagannath University, Jaipur**
**[2] Assistant Professor Faculty of Law Jaipur Jagannath University, Jaipur**

**ABSTRACT :**

Digital technology has transformed the nature of sexual offences, creating new forms of victimization through non-consensual dissemination of intimate images, cyberstalking, online sexual harassment, cyberflashing, impersonation, and technology-facilitated sexual exploitation. However, the harm caused by digital sex crimes does not necessarily end with the original offence. Victims may experience *secondary victimization* when they approach law enforcement authorities, participate in judicial proceedings, interact with digital platforms, or encounter insensitive treatment from society. Repeated questioning, victim-blaming, unnecessary disclosure of intimate material, delays in investigation, and the circulation of identifying information may compound the original injury. In India, constitutional protections, criminal law, procedural safeguards, information technology legislation, and judicial principles provide a framework for addressing these concerns. Nevertheless, the practical effectiveness of these protections depends on sensitive investigation, privacy-preserving evidence management, prompt removal of unlawful content, and a victim-centred approach to litigation. This paper examines the meaning, causes, legal dimensions, and consequences of secondary victimization in digital sex crimes, with particular reference to Indian law. It also analyses institutional challenges and proposes reforms to ensure that access to justice does not expose victims to further humiliation, discrimination, or psychological harm.

**Keywords: Secondary victimization, cybercrime, digital sexual abuse, online harassment, victim rights, privacy, evidence, Indian criminal law.**

## INTRODUCTION

The expansion of social media, messaging applications, image-sharing websites, artificial intelligence tools, and other digital technologies has created new opportunities for communication but has also facilitated sexual abuse and gender-based violence. Digital sex crimes include the non-consensual sharing of intimate images, online sexual harassment, cyberstalking, sexually explicit threats, the circulation of manipulated intimate imagery, and the creation or dissemination of sexual deepfakes. These offences can affect a victim's dignity, autonomy, privacy, mental well-being, professional life, and personal relationships. Unlike many conventional offences, digital abuse may continue long after the initial act because content can be copied, reposted, downloaded, and circulated across multiple platforms and jurisdictions.[1]

Secondary victimization occurs when a person who has already suffered harm experiences further injury through the responses of institutions, legal processes, social networks, or other individuals. In digital sex crime litigation, this may arise when police officers dismiss a complaint, investigators repeatedly require a victim to recount intimate experiences, lawyers use humiliating questioning, courts permit unnecessary disclosure of sensitive information, or online platforms fail to prevent continued circulation of abusive material. It may also occur when victims are blamed for creating intimate images, using particular applications, or trusting another person. The central concern is that the process intended to provide justice may inadvertently reproduce the victim's loss of control and dignity.[2]

The problem is particularly significant because successful prosecution often depends on digital evidence, including screenshots, account identifiers, messages, metadata, URLs, and forensic copies of electronic devices. Although such evidence may be necessary to establish the offence, its collection and presentation must be proportionate, lawful, and sensitive to privacy. An investigation that unnecessarily exposes intimate material or allows identifying information to circulate can create additional harm. Accordingly, effective online abuse litigation requires a balance between the accused person's right to a fair trial, the victim's rights to dignity and privacy, and the public interest in the effective administration of criminal justice.[3]

1 United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), Strategy: Preventing and Eliminating Technology-Facilitated Violence Against Women and Girls (2025
2 United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), Understanding and Measuring Technology-Facilitated Violence Against Women for Better Prevention and Response (7 July 2023).
3 United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), How AI Is Exacerbating Technology-Facilitated Violence

**RESEARCH OBJECTIVES**

The principal objectives of this research paper are:

1. To examine the concept and nature of secondary victimization in digital sex crimes.
2. To identify the institutional, procedural, technological, and social factors that contribute to secondary victimization.
3. To analyse the constitutional, statutory, and judicial framework applicable in India.
4. To evaluate the challenges associated with digital evidence, privacy, and victim participation in online abuse litigation.
5. To recommend legal and institutional reforms that promote victim-sensitive and fair judicial proceedings.

## RESEARCH METHODOLOGY

The present study adopts a doctrinal and analytical research methodology. It relies on primary legal sources, including the Constitution of India, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023. Relevant judicial decisions and established scholarship on victimology, privacy, sexual violence, and technology-facilitated abuse are also considered. The research is qualitative in nature and seeks to evaluate the adequacy of existing legal safeguards rather than to measure victim experiences through empirical fieldwork. The analysis focuses primarily on India while drawing on international human rights principles where useful for comparison.

**Meaning and Nature of Secondary Victimization**

Secondary victimization, sometimes described as second-order victimization, refers to additional harm experienced by a victim because of the manner in which other people or institutions respond to the original offence. In criminal justice, it may result from insensitive interviewing, disbelief, discriminatory treatment, repeated testimony, inadequate protection, or the disclosure of confidential information. In digital sexual abuse cases, the concept assumes particular importance because the victim may lose control over intimate information even after reporting the offence. The legal process should therefore avoid reproducing the very conditions of humiliation, exposure, and powerlessness that the original offender created.[4]

Secondary victimization may be direct or indirect. Direct secondary victimization occurs through the conduct of police personnel, prosecutors, defence counsel, judicial officers, medical professionals, or platform representatives. Indirect secondary victimization arises when victims encounter hostile media coverage, online ridicule, public speculation, family pressure, or repeated redistribution of intimate material. These experiences may overlap. For example, a victim who reports the non-consensual circulation of an intimate image may be required to provide multiple copies of the material, face questions about why the image was originally created, and subsequently discover that identifying details have appeared in public discussion.[5]

It is important to distinguish legitimate procedural safeguards from secondary victimization. An accused person must be permitted to challenge the prosecution's evidence, test the credibility of witnesses, and receive a fair trial. Nevertheless, these rights do not justify irrelevant, degrading, discriminatory, or unnecessarily intrusive questioning. The proper legal objective is not to eliminate scrutiny but to ensure that scrutiny remains relevant, proportionate, and consistent with dignity, privacy, and procedural fairness.

## MAJOR FORMS OF DIGITAL SEX CRIMES AND ONLINE ABUSE

**Non-consensual dissemination of intimate images**

Non-consensual dissemination of intimate images occurs when photographs, videos, or other intimate material are shared or published without the consent of the person depicted. The original material may have been created consensually, obtained through deception, or stolen from a device or account. Consent to create or privately share an image does not automatically constitute consent to publish it publicly. Victims may experience reputational damage, emotional distress, professional discrimination, threats, and continuing fear that the material will reappear. Litigation can aggravate this harm when intimate content is reproduced unnecessarily in complaints, pleadings, exhibits, or public reporting.[6]

**Cyberstalking and online sexual harassment**

Cyberstalking may involve persistent monitoring, unwanted communications, threatening messages, impersonation, or attempts to control another person's digital activities. Online sexual harassment may include sexually explicit remarks, unsolicited sexual content, coercive demands, and threats to publish private information. The repeated and borderless nature of digital communication can make it difficult for victims to escape the perpetrator. Secondary victimization arises when authorities treat the conduct as insignificant, suggest that the victim simply abandon social media, or fail to

Against Women and Girls (November 2025)

[4] . United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), Technology-Facilitated Violence Against Women: Taking Stock of Evidence and Data Collection (2023).

[5] United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), Technology-Facilitated Violence Against Women and Girls: Expert Group Meeting Report (2023).

[6] Information Technology Act, 2000, No. 21 of 2000, ss. 66E, 67 and 67A.

recognise the connection between online threats and possible physical danger.[7]

**Deepfake pornography and synthetic sexual imagery**

Artificial intelligence has increased the ability to create manipulated images, videos, and audio that falsely depict an individual in sexual situations. Such content may be fabricated without any authentic intimate photograph of the victim. Nevertheless, the victim can suffer serious reputational, psychological, social, and professional consequences. The circulation of synthetic sexual imagery raises questions about consent, identity, authenticity, platform accountability, and the preservation of digital evidence. Secondary victimization occurs when victims are asked to demonstrate the falsity of an image in humiliating ways, are blamed for its existence, or are required to repeatedly view and identify abusive content.[8]

**Sextortion and technology-facilitated coercion**

Sextortion involves threats to disclose intimate images, sexual information, or other sensitive material unless the victim provides money, further images, sexual acts, or some other demanded benefit. Perpetrators may exploit existing intimate relationships, hacked accounts, fabricated profiles, or deceptive online interactions. Victims may delay reporting because they fear exposure, criminalization, family rejection, or professional consequences. If authorities respond with suspicion or moral judgment, the resulting secondary victimization can reinforce silence and allow the perpetrator to continue the abuse.[9]

## CONSTITUTIONAL AND STATUTORY FRAMEWORK IN INDIA

**Constitutional protection of dignity and privacy**

Article 21 of the Constitution of India protects life and personal liberty, and its judicial interpretation encompasses dignity, privacy, and important aspects of personal autonomy. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognised privacy as a constitutionally protected right. This principle is significant in digital sexual abuse litigation because intimate information, personal communications, and sexual identity are closely connected with individual autonomy. Unnecessary exposure of a victim's identity or intimate material may undermine dignity even where disclosure is not essential to establishing guilt.[10]

Article 14 guarantees equality before the law and equal protection of the laws. Article 15 prohibits specified forms of discrimination, while Article 19 protects freedoms subject to constitutionally permissible restrictions. Together, these provisions inform the requirement that institutions respond to sexual abuse without gender stereotypes or arbitrary discrimination. A victim should not receive inferior protection because of social status, occupation, relationship history, online activity, or the consensual creation of intimate material. Constitutional guarantees must, however, be applied in their proper legal context and balanced against the rights of other parties.[11]

**Bharatiya Nyaya Sanhita, 2023**

The Bharatiya Nyaya Sanhita, 2023 (BNS), which came into force on 1 July 2024, provides several offences relevant to sexual and technology-facilitated abuse. Section 75 addresses sexual harassment; section 77 concerns voyeurism; section 78 addresses stalking, including specified monitoring of a woman's use of the internet, email, or other electronic communication; and section 79 concerns words, gestures, or acts intended to insult the modesty of a woman. Section 351, dealing with criminal intimidation, may also be relevant where the facts satisfy its requirements, including in cases involving threats to publish intimate material. The precise provision applicable depends on the conduct, statutory elements, evidence, and circumstances of the case.[12]

Section 77 is particularly relevant where a person watches, captures, or disseminates an image of a woman engaging in a private act in circumstances covered by the statutory definition. The provision also recognises that consent to capture an image does not necessarily imply consent to its dissemination. However, not every non-consensual intimate image case will automatically satisfy the elements of voyeurism. The prosecution must establish the statutory requirements, and other provisions of criminal and information technology law may be relevant depending on how the material was obtained or distributed.

Section 72 of the BNS penalises the unauthorised printing or publication of the identity of a victim of specified sexual offences, subject to statutory exceptions. This protection is important because identifying information may expose victims to stigma, threats, and further harassment. However, its scope is tied to the offences specified in the provision and should not be inaccurately treated as a universal anonymity rule covering every form of online abuse. Additional protections may arise under other legislation, procedural rules, and judicial directions.

**Information Technology Act, 2000**

[7] The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, ss. 75 and 78.
[8] UN Women, How AI Is Exacerbating Technology-Facilitated Violence Against Women and Girls, supra note 3.
[9] United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), Accelerating Efforts to Tackle Online and Technology-Facilitated Violence Against Women and Girls (2022).

[10] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[11] The Constitution of India, arts. 14, 15, 19 and 21.
[12] The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, ss. 75, 77–79 and 351.

The Information Technology Act, 2000 (IT Act) provides an important statutory framework for certain forms of digital sexual abuse. Section 66E penalises the violation of privacy through capturing, publishing, or transmitting images of a person's private area in circumstances specified by the provision. Section 67 addresses the publication or transmission of obscene material in electronic form, while section 67A concerns material containing sexually explicit acts or conduct. Section 67B deals with specified electronic material depicting children in sexually explicit acts or conduct, alongside related prohibited activities. The application of these provisions depends on their respective elements and the facts of the case.[13]

The IT Act is particularly important because digital sexual abuse frequently involves the electronic publication or transmission of material. Nevertheless, its provisions should not be interpreted as making every intimate image, private communication, or sexual representation automatically unlawful. The nature of the content, consent, statutory definitions, applicable exceptions, and the conduct of the accused must be examined. A victim-sensitive legal response must provide effective remedies without unnecessarily criminalising consensual adult expression or disregarding legitimate legal defences.

**Criminal procedure and evidentiary safeguards**

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) govern important aspects of criminal procedure and evidence. The BNSS provides procedural protections relevant to the recording of information and statements, investigation, and trial. Its provisions concerning specified sexual offences include safeguards relating to the recording of information and statements in appropriate circumstances. The BSA recognises electronic and digital records within the law of evidence and provides rules governing their admissibility and proof. Together, these enactments make it necessary to collect and present electronic evidence lawfully while preserving its authenticity and integrity.[14]

The evidentiary importance of screenshots, metadata, message histories, and forensic copies should not justify unlimited access to a victim's private digital life. Investigators should identify the material relevant to the alleged offence and avoid unnecessary examination or disclosure of unrelated intimate communications. Appropriate procedures for preserving original records, documenting the chain of custody, limiting access, and redacting irrelevant personal information can strengthen evidentiary reliability while reducing additional harm. The precise requirements of admissibility and certification must be assessed under the applicable provisions of the BSA.[15]

## JUDICIAL APPROACH TO PRIVACY, DIGNITY AND VICTIM PROTECTION

**State of Punjab v. Gurmit Singh**

In State of Punjab v. Gurmit Singh, the Supreme Court emphasised the need for sensitivity in the judicial treatment of victims of sexual offences. The judgment recognised the importance of avoiding approaches that discourage victims from participating in criminal proceedings. Although the case arose before the emergence of contemporary digital sexual abuse, its underlying principles remain relevant. Courts dealing with online abuse must assess evidence carefully while avoiding stereotypes, unnecessary humiliation, and assumptions that a victim's conduct automatically undermines credibility.[16]

**Nipun Saxena v. Union of India**

In Nipun Saxena v. Union of India, the Supreme Court addressed the protection of the identity of victims of sexual offences. The Court emphasised the need to prevent disclosure of information capable of identifying victims and clarified the importance of safeguarding their dignity and privacy. These principles are especially relevant in digital litigation, where names, photographs, locations, workplace details, and other identifying information can be combined to reveal a person's identity even when the name itself is withheld. Courts and media organisations should therefore assess identification risks comprehensively rather than relying exclusively on formal anonymity.[17]

**K.S. Puttaswamy v. Union of India**

The decision in Justice K.S. Puttaswamy (Retd.) v. Union of India provides the constitutional foundation for understanding privacy as an essential aspect of liberty and dignity. In online sexual abuse cases, privacy is not merely a question of concealing personal information; it also concerns the individual's control over intimate data and protection against unjustified intrusion. This principle supports proportionate evidence collection, confidential handling of sensitive material, and careful consideration of whether public disclosure is necessary for a fair hearing.[18]

These judgments should not be understood as establishing that every digital sexual abuse case must be conducted entirely in private or that the accused cannot challenge the prosecution's evidence. Rather, they support an approach in which privacy restrictions, anonymity, and protective measures are

[13] Information Technology Act, 2000, No. 21 of 2000, ss. 66E, 67, 67A and 67B.
[14] The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023; The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023.

[15] The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, provisions concerning electronic and digital records.

[16] State of Punjab v. Gurmit Singh, (1996) 2 SCC 384.
[17] Nipun Saxena v. Union of India, (2019) 2 SCC 703.
[18] . Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

determined according to applicable law and the circumstances of the case. The objective is to protect the victim against avoidable exposure while preserving judicial transparency, evidentiary scrutiny, and the rights of the accused.[19]

## CAUSES OF SECONDARY VICTIMIZATION IN ONLINE ABUSE LITIGATION

**Victim-blaming and gender stereotypes**

Victim-blaming remains a significant barrier to justice. Questions about why a victim shared an intimate image, maintained a relationship with the accused, responded to messages, or delayed filing a complaint may shift attention away from the alleged unlawful conduct. Such circumstances may occasionally be relevant to specific factual issues, but they should not be used to presume consent to subsequent dissemination or to justify harassment. A sound legal approach distinguishes the victim's previous conduct from the legal elements of the alleged offence.[20]

**8.2 Repeated interviews and insensitive investigation**

Repeated interviews may require victims to recount distressing experiences to several police officers, forensic specialists, prosecutors, and other professionals. Differences in recollection, especially concerning peripheral details, may then be treated unfairly as evidence of dishonesty. Investigative authorities should coordinate interviews where practicable, explain why further questioning is necessary, use trained personnel, and avoid unnecessarily graphic or repetitive questioning. Such measures can improve both victim welfare and the quality of evidence collected.[21]

**Digital evidence exposure and privacy violations**

Electronic evidence presents a distinctive risk because sensitive content can be duplicated with minimal effort. Intimate images submitted to establish an offence may be copied into multiple files, forwarded through unofficial channels, or displayed to persons who have no legitimate need to view them. Even when the original material is essential evidence, unrestricted access creates further opportunities for humiliation and dissemination. Secure storage, access controls, redaction, forensic documentation, and reasoned judicial directions are therefore essential components of responsible evidence management.

**Delay, lack of coordination and inadequate remedies**

Delays in identifying perpetrators, obtaining platform records, removing unlawful content, and completing investigations can extend the period of victimization. Digital content may be reposted repeatedly while jurisdictional disputes or procedural obstacles remain unresolved. Victims may also be required to approach several institutions without receiving clear information about available remedies. Effective coordination between police, forensic laboratories, prosecutors, courts, and online intermediaries can reduce these difficulties and improve confidence in the justice system.[22]

**Challenges in Online Abuse Litigation**

A major challenge is the cross-border nature of digital offences. The victim, accused, hosting platform, server, and relevant data may be situated in different jurisdictions. Preservation requests, disclosure of account information, and international cooperation may therefore take time. In addition, encryption, anonymous accounts, deleted content, and rapidly changing technologies can complicate investigation. These difficulties require specialised technical capacity and effective cooperation, but they must not become reasons for dismissing complaints or shifting the entire burden of investigation onto victims.[23]

A second challenge concerns the balance between privacy and the right to a fair trial. The accused must be able to understand and challenge the evidence relied upon by the prosecution. At the same time, unrestricted disclosure of intimate material may expose victims to serious harm. Courts should consider whether evidence can be presented through redacted documents, restricted access, secure electronic exhibits, or other lawful protective measures. Such arrangements must be consistent with procedural law and should not prevent the defence from receiving the material necessary to contest the prosecution's case

A third challenge is the evolving nature of artificial intelligence-generated abuse. Synthetic imagery may be created from publicly available photographs, and determining its origin may require specialist analysis. Content moderation systems may also fail to distinguish between unlawful sexual abuse, legitimate reporting, and consensual adult material. Consequently, legal and technical responses must combine accurate evidence assessment, clear reporting procedures, proportionate restrictions, and appropriate human review. The absence of a single comprehensive solution makes coordination between legal institutions, technology companies, and victim-support organisations particularly important.[24]

---

[19] Nipun Saxena v. Union of India, (2019) 2 SCC 703.
[20] State of Punjab v. Gurmit Singh, (1996) 2 SCC 384.
[21] United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), Technology-Facilitated Violence Against Women and Girls: Expert Group Meeting Report (2023).
[22] UN Women, Strategy: Preventing and Eliminating Technology-Facilitated Violence Against Women and Girls, supra note 1.
[23] . UN Women, How AI Is Exacerbating Technology-Facilitated Violence Against Women and Girls, supra note 3.
[24] The Constitution of India, art. 21; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

## 10. Recommendations and Legal Reforms

First, victim-sensitive investigation should become an institutional priority. Police personnel, prosecutors, judicial officers, and digital forensic professionals should receive specialised training on technology-facilitated sexual abuse, trauma-informed interviewing, gender sensitivity, and privacy protection. Standard operating procedures should encourage coordinated interviews, clear explanations of legal processes, and the avoidance of unnecessary repetition. Training must also emphasise that consent to create or privately share intimate material does not automatically establish consent to its further distribution.

Second, confidential handling of digital evidence should be strengthened. Investigating agencies should adopt secure procedures for receiving, preserving, transferring, and examining intimate digital material. Access should be restricted to authorised persons with a legitimate professional need. Copies should be made only when necessary, and sensitive exhibits should be protected against unauthorised downloading or onward transmission. Courts should consider appropriate redaction, restricted inspection, and confidentiality directions wherever permitted by law, while maintaining the evidentiary access necessary for a fair trial.[25]

Third, content-removal mechanisms should be accessible and effective. Victims should be able to report non-consensual intimate imagery, impersonation, and sexual deepfakes through clear and responsive complaint systems. Intermediaries should provide understandable procedures, acknowledge complaints, preserve relevant evidence where legally appropriate, and comply with applicable removal and disclosure obligations. Removal should be accompanied, where feasible, by measures to limit repeated uploads and protect the complainant's identity. Such systems should incorporate safeguards against mistaken removal and abuse of reporting mechanisms.

Fourth, legal assistance and psychological support should be integrated into the justice process. Victims may need counselling, legal representation, information about procedural rights, and assistance in dealing with digital platforms. Access to support should not depend entirely on a victim's financial resources or technical knowledge. Appropriate referrals through legal services authorities, victim-support organisations, and other competent institutions can make reporting less intimidating and reduce the likelihood that victims abandon proceedings because of procedural burdens.[26]

Fifth, courts should adopt proportionate protective measures. Depending on the applicable law and facts, these may include in-camera proceedings, restrictions on identifying information, secure access to intimate exhibits, and directions against unnecessary publication. The court should explain the basis and scope of protective measures and periodically consider whether they remain necessary. Such safeguards must not become a substitute for proper evidence evaluation or prevent the accused from exercising legitimate defence rights.[27]

Sixth, a coordinated regulatory approach is necessary. The government should periodically review the interaction between criminal law, information technology regulation, privacy protections, evidence rules, and victim compensation mechanisms. Clear protocols for urgent preservation of digital evidence, inter-agency referrals, and cross-border cooperation can reduce delay. Research and reliable data collection should also be strengthened, with appropriate confidentiality safeguards, to identify where victims experience the greatest barriers to reporting and redress.

## CONCLUSION

Secondary victimization in digital sex crimes represents a serious challenge to the effective administration of justice. Non-consensual dissemination of intimate images, cyberstalking, sexual harassment, sextortion, and AI-generated sexual imagery can cause profound harm because digital content may remain accessible and be redistributed long after the original incident. When victims encounter disbelief, degrading questioning, unnecessary disclosure, procedural delays, or insensitive platform responses, the resulting harm extends beyond the initial offence. A justice system must therefore evaluate its success not only by the number of prosecutions or convictions but also by whether its procedures protect dignity, privacy, fairness, and meaningful access to remedies.

The Indian legal framework provides several relevant protections through Articles 14 and 21 of the Constitution, the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023. Judicial decisions concerning privacy and the protection of sexual-offence victims further inform the interpretation and application of these laws. Nevertheless, the existence of statutory provisions does not automatically prevent secondary victimization. Effective implementation requires trained personnel, secure evidence-management practices, proportionate confidentiality measures, timely investigation, and accessible support services.

Ultimately, the objective of victim-sensitive litigation is not to weaken the presumption of innocence or restrict legitimate defence rights. It is to ensure that the pursuit of truth does not unnecessarily reproduce the harm caused by the alleged offence. A balanced system should protect victims from avoidable exposure, preserve reliable evidence, ensure fair hearings, and hold perpetrators accountable under applicable law. By integrating constitutional dignity, technological responsibility, procedural fairness, and institutional sensitivity, India can strengthen its response to digital sexual

[25] Information Technology Act, 2000, No. 21 of 2000; The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023.
[26] Legal Services Authorities Act, 1987, No. 39 of 1987; Council of Europe, Recommendation on Accountability for Technology-Facilitated Violence Against Women and Girls (2026).
[27] Nipun Saxena v. Union of India, (2019) 2 SCC 703; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

abuse and build a justice system in which seeking legal protection does not become another source of victimization.

**BIBLIOGRAPHY**


1. Ahlawat, Manu. "Cyber Violence Against Women: Emerging Legal Challenges and the Need for Gender-Sensitive Digital Protection Laws." Indian Journal of Law, vol. 4, no. 4, 2026. https://doi.org/10.36676/ijl.v4.i4.197.
2. Dey, Adrija. "'It's a Joke, Not a Dick. So Don't Take It Too Hard': Online Sexual Harassment in Indian Universities." Feminist Media Studies, vol. 24, no. 8, 2024, pp. 1830–1846. https://doi.org/10.1080/14680777.2023.2266150.
3. Halder, Debarati, and Subhajit Basu. "Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India." Information & Communications Technology Law, vol. 34, no. 2, 2025, pp. 163–186. https://doi.org/10.1080/13600834.2024.2408914.
4. Johari, Avantika, and Purvi Pokhariyal. "Tracking Harm in the Shadows: Legal and Forensic Responses to the Dark Web Sexual Crimes in India." Journal of Applied Security Research, vol. 21, no. 3, 2026, pp. 470–506. https://doi.org/10.1080/19361610.2026.2680890.
5. Khanam, Humaira, and Krupa Nishar. "Beyond the Crime: Secondary Victimisation of Rape Survivors in India." International Journal of Law, Culture & Society, vol. 2, no. 2, 2026.
6. Lal, Disha, Udaya Kumar Giri, and Shrish Kumar Tiwari. "Virtual Vulnerability: Addressing Cyber Harassment against Women in India." DS Journal of Cyber Security, vol. 2, no. 3, 2024, pp. 1–14. https://doi.org/10.59232/CYS-V2I3P101.
7. Mohan, Chathuri C., and Febin Baby. "Women Victims of Cyber Sexual Harassment—A Study with Reference to Kerala, India." International Research Journal of Social Sciences, vol. 13, no. 4, 2024, pp. 13–21.
8. Paliwal, Gaurav, Nidhi Asthana, and Divya Gautam. "Unveiling the Cyber Landscape: Analysis of Cybercrimes Against Women in India and Future Directions." European Economic Letters, vol. 14, no. 2, 2024, pp. 1270–1286. https://doi.org/10.52783/eel.v14i2.1468.
9. Sarkar, Sahana, and Rahul Sinha-Roy. "Cybersecurity Through an Intersectional Lens: Survivors' Responses to Technology-Facilitated Sexual Violence in India." Feminist Criminology, published online, 29 November 2025. https://doi.org/10.1177/15570851251406560.
10. The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023), concerning criminal procedure and victim-related procedural protections.
11. The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), particularly the provisions concerning sexual harassment, voyeurism, stalking and other relevant offences.
12. The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023), concerning evidence, including electronic and digital records.
13. The Digital Personal Data Protection Act, 2023.
14. The Indecent Representation of Women (Prohibition) Act, 1986.
15. The Information Technology (Amendment) Act, 2008.
16. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
17. The Information Technology Act, 2000, especially §§ 66E, 67, 67A and 67B, as applicable to the conduct in question.
18. The Protection of Children from Sexual Offences Act, 2012.
19. Verma, Rajesh Kumar, and Deepak Chand. "Online Abuse Against Women in India: A Critical Legal Analysis of Cyber Harassment." International Journal of Emerging Technologies and Innovative Research, vol. 13, no. 8, 2026, pp. b650–b659.
20. Verma, Rajesh Kumar, and Deepak Chand. "Online Abuse Against Women in India: A Critical Legal Analysis of Cyber Harassment." International Journal of Emerging Technologies and Innovative Research, vol. 13, no. 8, August 2026, pp. b650–b659..