# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896




# LEGAL FRAMEWORK RELATED TO PRIVACY IN THE INTERNET ERA FOR WOMEN – WITH SPECIAL REFERENCE TO REVENGE PORN, BLACKMAILING, AND CYBER HARASSMENT


***~ Srishti Gupta***



## Abstract

In the digital era, the right to privacy has emerged as one of the most significant yet vulnerable aspects of human life, particularly for women. With the growing use of social media and online platforms, crimes such as revenge porn, blackmailing, cyberstalking, and harassment have created serious threats to women's dignity, autonomy, and security. These offences not only violate fundamental rights but also exploit technological loopholes and the anonymity of cyberspace, leaving women more exposed to psychological, social, and emotional harm.

This research focuses on the legal framework related to privacy in India, with special reference to the challenges faced by women in cyberspace. It examines constitutional protections under Article 21, statutory safeguards under the Indian Penal Code and Information Technology Act, and the role of judiciary in expanding the scope of privacy as a fundamental right. International perspectives, including conventions such as CEDAW and the Budapest Convention on Cybercrime, are also considered to highlight global standards and best practices. Through doctrinal and analytical methods, the study critically evaluates the adequacy of the existing laws in addressing crimes like revenge porn and cyber harassment, and identifies gaps in their implementation. It further aims to suggest reforms for stronger victim protection, efficient law enforcement, and greater digital awareness. Ultimately, the research underscores that safeguarding women's privacy in the internet era is not merely a legal necessity but also an essential step towards ensuring gender justice, equality, and human rights in the modern world.



## Keywords

Revenge Porn, Cyber Harassment, Online Blackmailing, Gender Justice, Cyber stalking, Data Protection, Online Safety.


## Introduction

In today's digital society, the internet has become an essential platform for communication, financial transactions, social networking, political participation, and entertainment. While it has improved efficiency, it has also created serious risks to personal privacy. Individuals—particularly women—are vulnerable to misuse of private information, including financial

details, personal conversations, medical data, intimate images, etc. Such privacy violations can result in identity theft, blackmailing, cyberbullying, harassment, and reputational damage. Privacy, therefore, is a necessity in the modern world, recognized as a fundamental right under Article 21 of the Indian Constitution [1](Justice K.S. Puttaswamy v. Union of India, 2017). In the internet era, privacy has become a fundamental need, as individuals often share sensitive personal, financial, and social information online through social media, mobile applications, and browsing activities. Misuse of such data can lead to identity theft, financial fraud, cyber bullying, blackmailing, and circulation of intimate content (revenge porn).

In the internet era, many types of private data are at risk, including financial information, personal conversations, medical records, intimate photos or videos, identity details, location data, professional documents, browsing history, and contact information. If leaked, this data can lead to fraud, harassment, blackmail, identity theft, stalking, or corporate misuse. Old devices with stored personal data are also vulnerable. These risks highlight the importance of strong privacy protections, especially for women who are often more vulnerable to online exploitation.

Threatening an individual with the disclosure of their private information for personal gain, such as money or Favors, is known as blackmailing. When such threats are carried out through digital means like emails, social media, or messaging apps, it is called online blackmailing. A severe form of this is sextortion, where private or intimate images are misused to demand sexual Favors or money. Women are the victims of these types of crimes, and such crimes remain unreported to maintain the reputation in the society. In [2]Ved Prakash v. State of UP (2010) case, the accused secretly took a woman's nude photos and blackmailed her, leading to sexual assault. The Court emphasized that such acts are a gross invasion of privacy and dignity, highlighting the need for strong legal protection for women against online blackmail and sextortion.

Revenge porn refers to the distribution of sexually explicit images or videos of a person without their consent, typically to harass, embarrass, or exert control over them. While often committed by former intimate partners, the key aspect is the lack of consent and the violation of privacy, regardless of the perpetrator's motive. Scholars argue that the term "revenge porn" can be misleading, as revenge is not always the intent, and propose alternative terms like non-consensual pornography or involuntary pornography.

This phenomenon is distinct from consensual pornography, where both creation and sharing are agreed upon, and from other forms of non-consensual pornography, such as voyeuristic images or hacked content. In some cases, images are shared by third parties without malice, which is sometimes called uninvolved revenge pornography. What makes revenge porn

[1]Justice K.S. Puttaswamy v. Union of India, 2017 Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161 last visit on 03.09.2025

[2]Ved Prakash And Another vs. State Of U.p. & OthersWRIT – B No. - 3060 of 2023 | 29-01-2024 last visit on 03.09.2025

particularly harmful is the breach of trust between partners, which can have devastating emotional and social consequences. Revenge porn often targets women because intimate images or videos of women are more likely to be misused to shame, humiliate, or exert control. Patriarchal social norms frequently judge women more harshly for sexual content than men. Revenge porn often targets women because intimate images or videos of women are more likely to be misused to shame, humiliate, or exert control. Patriarchal social norms frequently judge women more harshly for sexual content than men. Women victims are often subjected to online shaming, cyber bullying, or harassment, which can affect personal, social, and professional life. This societal blame disproportionately falls on women due to gendered norms around sexuality.

Revenge porn[3] is defined as sexually exploited images of a person posted online without the person's knowledge or any content in the form of revenge and harassment and embarrassment. Without the subject's agreement and in order to cause them distress or embarrassment, revealing or sexually explicit photographs or videos of them are released on the Internet, generally by a former sexual partner. sexually suggestive photographs of someone, usually a former love partner, that are shared without the person's consent online or otherwise. This definition will not be utilized here since they are unclear about the activity that has been agreed to and focus on the notion of "revenge. "The term "revenge pornography," as employed in this thesis, refers to a circumstance in which personal relationships are retaliated against. The photographs or films used in revenge pornography were likely taken or shared during a private encounter or relationship. This is particularly crucial because these interactions or relationships are typically assumed to be fully private. In contrast to consensual pornographic interactions and relationships.

Victims of revenge porn often suffer humiliation, harassment, mental trauma, and social ostracism. High-profile cases, such as Suchitra Gupta in India and Tiziana Cantone in Italy, demonstrate the extreme psychological impact, including suicidal attempts. Legal interventions, such as the right to be forgotten, can help remove such content online, but the legal and social challenges remain significant.

Overall, revenge porn underscores the critical need for robust legal protections, awareness, and digital literacy to safeguard privacy, particularly for women, in the internet era.

## LITERATURE REVIEW

The digital revolution has brought numerous conveniences but has simultaneously exposed women to risks related to privacy breaches, cyber harassment, and online exploitation. Scholars, policymakers, and legal experts have extensively studied the threats posed by the internet to personal privacy and the legal mechanisms to counter them.

[3] Author Goudsmith, M. A. R. T. H. E. published on 2017, February 16. https://www.researchgate.net/publication/324360144_Revenge_pornography_A_conceptual_analysis_Undressing_a_crime_of_disclosure last visited on 04.09.2025

**1. Internet Privacy and Data Vulnerability:-** According to [4]DANIEL J. Solove (2008), personal information in the digital era is highly vulnerable due to data collection by social media, mobile applications, and online services. Privacy risks include financial fraud, identity theft, and unauthorized sharing of personal data. Research by Acquisti et al. (2015) highlights that users often underestimate the extent to which personal information is exposed online, making them susceptible to exploitation. In India, studies by Sahu & Singh (2019) emphasize that the lack of comprehensive data protection laws further endangers sensitive personal information, particularly that of women.

**2. Revenge Porn and Non-Consensual Sharing:-** Scholars such as [5]Henry & Powell (2016) define revenge porn as the non-consensual sharing of intimate images, typically by former partners, to humiliate or control the victim. Scheller (2017) suggests using the term "non-consensual pornography" to emphasize the violation of consent rather than focusing solely on revenge motives. Research indicates that women are disproportionately affected by revenge porn, experiencing psychological trauma, social stigma, and reputational damage (Bates, 2017). Cases like Tiziana Cantone in Italy and Suchitra Gupta in India underscore the global prevalence and severe consequences of such violations.

**3. Blackmailing and Sextortion:** Blackmailing and sextortion involve threatening individuals, usually women, with exposure of private or intimate content to extract money, sexual favors, or other benefits. Literature by Whitty & Young (2018) highlights that women are often targeted due to power imbalances and societal vulnerability. Indian case law, such as Ved Prakash v. State of UP, demonstrates the intersection of sexual exploitation and digital blackmail, illustrating the real-world implications of these crimes.

**4. Cyber Harassment and Online Abuse:** Cyber harassment encompasses stalking, trolling, and abusive messages that compromise women's safety and autonomy online. Studies by [6]Patchin & Hinduja (2017) emphasize the psychological impact of cyber harassment, noting increased anxiety, depression, and social withdrawal among female victims. Research in the Indian context ([7]Kaur & Singh, 2020) points out that social media platforms are frequently misused to target women, often exploiting loopholes in legal enforcement.

**5. Legal Framework and Challenges:** The Indian legal system primarily relies on the Information Technology Act, 2000, and its amendments, along with provisions of the Indian Penal Code (IPC), to address cybercrimes. Scholars such as Dahiya (2018) argue that while these laws provide some protection, they are

[4]Author Daniel j. solove 2008 " internet privacy and data vulnerability (last visited on 04.09.2025) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

[5]Henry & Powell (2016) Revenge Porn and Non-Consensual Sharing (last visited on 09.09.2025) https://pubmed.ncbi.nlm.nih.gov/27311818/

[6] Patchin & Hinduja (2017) Cyber Harassment and Online Abuse (last visited on 09.09.2025) http://jahonline.org/retrieve/pii/S1054139X17303130

[7]Author Kaur & Singh, 2020 on cyber harassment and online abuse (last visited on 09.09.2025) https://www.scirp.org/reference/referencespapers?referenceid=3624571

insufficient to address the nuances of revenge porn, sextortion, and persistent online harassment. The lack of specific legislation on non-consensual pornography and the challenges of cross-border cybercrime limit effective enforcement.

India's legal framework comprises provisions from the Information Technology Act, 2000, and the Indian Penal Code (IPC), recently revised under the Bharatiya Nyaya Sanhita (BNS), 2023.

Section 66E of the IT Act penalizes the violation of privacy through capturing and sharing private images.

Sections 67 and 67A of IT Act deal with obscene and sexually explicit content in electronic form.

Under the IPC/BNS, Sections 354C (voyeurism) and 354D (cyberstalking) are frequently invoked in such cases.

According to Bhadoria (2023), while these laws exist, they often lack clarity on newer threats like AI-generated deepfakes, fake profiles, and organized doxxing. Furthermore, the Digital Personal Data Protection Act, 2023, though a step forward, has limited enforcement mechanisms and an ambiguous grievance redressal system (Sharma, 2024).

**[8]Consent and Sexual Relations**

According to scholar Wertheimer (2018) emphasizes that privacy, particularly sexual privacy, is a subset of bodily autonomy and personal dignity. In the digital age, the non-consensual dissemination of intimate images — often called "revenge porn" — violates this fundamental right. [9]Citron and Franks (2014) argue for retiring the term "revenge porn" in Favor of "non-consensual pornography" or "image-based sexual abuse" (IBSA), which better captures the spectrum of digital harms beyond a retaliatory motive.

[10]Patel (2021) notes that online abuse is a continuation of offline gender-based violence, with digital spaces becoming new arenas for misogyny, control, and shaming of women.

## 7. [11]NALSAR LAW REVIEW REPORT

According to the Empirical studies done by the author in this report indicate low reporting rates for digital sexual violence due to stigma, fear of retaliation, and lack of trust in law enforcement (author Agarwal & Singh, 2021). A survey by Internet Democracy Project (2022) found that over 70% of women do not pursue legal action even after serious online abuse.

---

[8]Author Wertheimer (2018) Consent and Sexual Relations Published online by Cambridge University Press: 16 February 2009 (last visited on 10.09.2025)

[9] Citron, Danielle Keats and Franks, Mary Anne, Criminalizing Revenge Porn (May 19, 2014). Wake Forest Law Review, Vol. 49, 2014, p. 345+, U of Maryland Legal Studies Research Paper No. 2014-1, Available at SSRN: https://ssrn.com/abstract=2368946 (last visited on 10.09.2025)

[10] Author Aayushi Patel (2021) Cyber Crimes in India: A Review Paper (page no. 5 – 14) (last visited on 11.09.2025) https://gem.sgcaruvithura.ac.in/assets/vol4-issue1/vol4-issue1-paper1.pdf

[11]Agrawal and Singh (2021) NALSAR LAW REVIEW REPORT https://nalsar.ac.in/images/NLR_Vol%208_No-2.pdf (last visited on 11.09.2025)

**8. [12]Cyber Crimes and Harassment of Women: Evaluating the Effectiveness of Legal Frameworks**

According to Author Shubham Verma, Law Centre-1, Faculty Of Law, University of Delhi in the year 2024, analyses cybercrimes against women—including cyberstalking, doxxing, revenge pornography, and deepfake abuse—and critiques the efficacy of India's legal framework under the IT Act and IPC. Verma notes the foundational strengths of existing laws, but underscores critical shortcomings: gaps in enforcement, limited public awareness, and technological limitations. Comparative insights drawn from the US VAWA and EU GDPR point to innovative responses that India could adapt.

**9. Addressing Judicial Issues in Revenge Porn Cases**

According to scholar Sanika Atul Jadhav outlines the socio-legal impact of revenge pornography in India. She notes the absence of a specific legal provision, forcing reliance on broad sections of the IT Act (Sections 66E, 67/67A) and IPC (Sections 500, 504, 506, 509, 354A, 354C). Scholar Sanika Atul Jadhav highlights both the psychological harm and societal fallout of such non-consensual image distribution.

**10. Revenge Pornography: Legal Framework in India**

[13]Prashant Mali (2021), in his IJLMH paper "Revenge Pornography: Legal Framework in India", explores the rising prevalence of non-consensual image-sharing driven by social media and anonymity. His study assesses India's legal tools and remedies for victims, while pointing to shortcomings like weak awareness, insufficient training, and the psychological profile of perpetrators.

**11. [14]Keeping women safe? Gender, online harassment and Indian law**

According to [15]scholar Richa Kaul Padte & Anja Kovacs (2013), through their brief "Keeping women safe? Gender, online harassment and Indian law," critique the shortcomings of Section 66A—which was often invoked for online verbal abuse—and point to its misuse as a censorship tool, ultimately struck down by the courts. The authors discuss the reluctance of

[12]Author Shubham Verma Cyber Crimes and Harassment of Women: Evaluating the Effectiveness of Legal Frameworks https://nyayanishtha.com/article/cyber-crimes-and-harassment-of-women-evaluating-the-effectiveness-of-legal-frameworks (last visited on 13.09.2025)

[13] Author Prashant Mali (2021), in his IJLMH paper "Revenge Pornography: Legal Framework in India"https://ijlmh.com/paper/revenge-pornography-legal-framework-in-india/ (last visited on 13.09.2025)

[14] Author Richa Kaul Padte & Anja Kovacs (2013), through their brief "Keeping women safe? Gender, online harassment and Indian law," https://internetdemocracy.in/wp-content/uploads/2013/04/Internet-Democracy-Project-Gender-Online-Harassment-and-Indian-Law.pdf (last visited on 13.09.2025)

[15] Author Richa Kaul Padte & Anja Kovacs (2013), through their brief "Keeping women safe? Gender, online harassment and Indian law," https://internetdemocracy.in/reports/keezing-women-safe-gender-online-harassment-and-indian-law/ (last visited on 13.09.2025)

women to seek legal recourse due to disbelief, blame, or fear—highlighting low trust in law enforcement and lack of legal literacy.

### 12. Female Abuse Through Social Networking Sites: A Critical Analysis of IT Act 2000

According to scholar [16]Meha Dad, Under "Female Abuse Through Social Networking Sites: A Critical Analysis of IT Act 2000," the scope of Section 66E and IPC Section 354C (Voyeurism) are examined, alongside the case of [17]Yogesh Prabhu v. State of Maharashtra (2015)—one of India's early cyberstalking cases involving unsolicited obscene content.

A detailed review in LegalServiceIndia covers cyberstalking, cyber defamation, morphing (manipulating images), trolling, email spoofing, and phishing. It underscores how women are disproportionately targeted and notes the limitations of laws like the IT Act and IPC, particularly in operational complexity and low awareness among stakeholders**.**

### 13. CYBER STALKING: - A DEAD TRAP

Swasti Sonar (Tezpur Law College) explores the updated legal landscape under the Bharatiya Nyaya Sanhita (BNS), 2023. Her research emphasizes Section 78 of BNS—which specifically defines cyberstalking and enforces stringent punishments. She also discusses AI's dual role, as a tool both for offenders (deepfakes) and for law enforcement capabilities.

### 14. International Journal for Legal Research and Analysis

According to scholar [18]Divya Yadav (International Journal for Legal Research and Analysis) addresses cyberbullying, particularly affecting young Indians. She points out the lacunae in current laws—IT Act and IPC sections are inadequate to address psychological harm and anonymity inherent in cyberbullying. Divya Yadav calls for standalone legislation and improved coordination with digital platforms and law enforcement.

[19]Aishwarya Sandeep highlights how the post-COVID digital boom in India has escalated cybersex, cyberpornography, sextortion, and image blackmail. She restates the roles of Section 66E, 67/67A and IPC Sections 354C/D, and cites the Cyber Crime Prevention Against Women and Children (CCPWC) initiative as a positive government intervention to improve reporting and capacity-building. A report on sextortion and revenge porn emphasizes alarming real-world outcomes—including suicides among victims—and details one landmark conviction in Midnapore, West Bengal. Despite applying multiple IT Act and IPC provisions, the punishment (five years imprisonment and ₹9,000 fine) still highlighted the absence of tailored laws for such crimes.

---

[16] https://www.legalserviceindia.com/legal/article-4112-female-abuse-through-social-networking-sites-a-critical-analysis-of-it-act-2000.html

[17] The State (Cyber Cell) v. Yogisha @ Yogesh Pandurang Prabhu r/o Vashi Citation: C.C. No. 3700686/PS/2009 Date of Judgement: 3rd July, 2015

[18] Author Divya Yadav (International Journal for Legal Research and Analysis) (page no. 7 – 15) https://www.ijlra.com/details/cyberbullying-laws-in-india-current-challenges-and-reforms-by-divya-yadav last visited on 25.09.2025

[19]Author Aishwarya Sandeep (2021) https://aishwaryasandeep.in/cyberspace-regulation-detailed-analysis-of-international-legal-framework/

[20]Debarati Halder (Unitedworld School of Law) critiques the absence of a specific law for revenge pornography in India. She argues that reliance on Section 66E (IT Act), Sections 354C/354D (IPC) fails to inspire police action or societal recognition—calling for a separate prohibition law.

### 15. International Responses

Globally, legal responses have varied in scope and effectiveness. The United States introduced the TAKE IT DOWN Act in 2025, mandating online platforms to remove non-consensual images within 48 hours. Additionally, states like California have enacted specific laws criminalizing the distribution of intimate images without consent (Franks, 2020).

The United Kingdom's Online Safety Act (2023) addresses NCII and cyberflashing, placing obligations on digital platforms. However, Lewis et al. (2024) criticize its vague provisions, arguing that it falls short in enforcing swift redressal for victims.

Australia's e- Safety Commission model has been hailed as a benchmark due to its centralized redressal mechanism and preventive tools like StopNCII.org ([21]Douglas & Burdon, 2022).

### 16. Judicial Precedence

Cases such as [22]Suhas Katti v. State of Tamil Nadu (2004) marked one of the earliest cyber harassment convictions in India. More recent cases like X v. Union of India (Madras HC, 2025) have highlighted the judiciary's evolving understanding of online privacy and the need for platform accountability.

In [23]K.S. Puttaswamy v. Union of India (2017), the Supreme Court recognized the right to privacy as a fundamental right under Article 21 of the Constitution. Scholars like Bhatia (2019) argue that this ruling provides the foundation for strengthening protections against NCII and cyber exploitation.

### 17. [24]Sulli Deals, Bulli Bai and the young and educated hatemongers (news report)

[20]Debarati Halder (Unitedworld School of Law) last visited on 25.09.2025 https://scholar.google.com/citations?view_op=view_citation&hl=en&user=DL3TANYAAAAJ&citation_for_view=DL3TANYAAAAJ:QIV2ME_5wuYC

[21] Douglas, Heather. (2018). Legal Responses to Non-Consensual Smartphone Recordings in the Context of Domestic and Family Violence. New South Wales Law Journal. 41. 1. 10.53637/RMSL3175. last visited on 25.09.2025

[22] Suhas Katti v. State of Tamil Nadu case from 2004 is CC No. 4680 of 2004 last visited on 25.09.2025

[23] Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017 last visited on 25.09.2025

[24] Alok Deshpande, Hemani Bhandari Sulli Deals, Bulli Bai and the young and educated hatemongers (news report) last visited on 04.10.2025 https://www.thehindu.com/news/national/sulli-deals-bulli-bai-and-the-young-and-educated-hatemongers/article38305009.ece

According to reporter Alok Deshpande, Hemani Bhandari, the Bulli Bai and Sulli Deals incidents (2021–22) exposed the failure of timely legal intervention and the complicity of digital platforms in enabling such harassment. Gupta (2022) criticizes the reactive nature of Indian cyber law enforcement and calls for stronger, proactive content moderation policies.

### Research Gaps

The literature indicates several gaps: inadequate legal definitions for emerging cybercrimes, limited awareness among women regarding digital privacy, insufficient digital literacy, and weak enforcement mechanisms. Researchers suggest the need for stricter legislation, victim-centric reporting mechanisms, public awareness campaigns, and collaboration between legal authorities and technology platforms to protect women online (Henry & Powell, 2018; Kaur, 2021).

## OBJECTIVES

- To examine the existing legal framework addressing privacy violations against women in cyberspace.
- To analyse the effectiveness criminal provisions dealing with revenge porn, blackmailing, and online abuse.
- To suggest reforms and policy measures for stronger protection of women in the internet era.

## RESEARCH QUESTION

- Analyse why the breach of privacy, private data, blackmailing and revenge porn occur and what are that criminal intention behind that.
- How do international conventions and foreign legal frameworks compare with India's approach to protecting women's digital privacy?
- Why crime against women remain unnoticed and unreported?
- Analyse the perspective of people regarding such serious crime related to women.

### Legal Framework in India

❖ **Information Technology Act, 2000 (IT Act)**

- **Section 66E** – Punishes violation of privacy through capturing, publishing, or transmitting images of private areas.
- **Section 67, 67A, 67B** – Penalizes publishing or transmitting obscene/sexually explicit material.
- **Section 69, 69A** – Empower the government to block objectionable content.

- **Bharatiya Nyaya Sanhita, 2023 (BNS)**
  - **Section 77** – Voyeurism.
  - **Section 78** – Stalking (including cyberstalking).
  - **Section 356(1) and 356(2)** – Defamation through online circulation of images.
  - **Section 79** – Word, gesture, or act intended to insult the modesty of a woman.
  - **Section 294& 296** – Obscenity provisions.
  - **Section 308(2)** – Punishment for blackmail and extortion.
- **Constitutional Safeguards**
  - **Article 21** – Right to life and personal liberty includes the right to privacy and dignity.
  - **Article 19(1)(a)** – Freedom of speech balanced with restrictions under **Article 19(2)**.
- **Judicial Precedents related to cyber crime**
  - [25]*Justice K.S. Puttaswamy v. Union of India (2017)* – Recognized privacy as a fundamental right.
  - [26]*Shreya Singhal v. Union of India (2015)* – Struck down Section 66A IT Act but highlighted state's duty to regulate harmful online content.
  - *Avnish bajaj vs state (2005)* - This case underscored the need for clear guidelines on intermediary liability to prevent the dissemination of obscene content, including revenge pornography, which disproportionately affects women. It prompted amendments to the IT Act to strengthen protections against such cybercrime.

## METHODOLOGY

The present study is mixed research in nature and relies primarily on qualitative analysis of legal texts, judicial decisions, and academic writings. Primary sources such as the Constitution of India, particularly Article 21 on the right to privacy, provisions of the Indian Penal Code, and the Information Technology Act, 2000 with its subsequent amendments, have been examined to understand the statutory framework and also empirical method for which I rely on the questionnaire which is being shared among the people of all age groups. Landmark judgments including Justice K.S. Puttaswamy v. Union of India and Shreya Singhal v. Union of India are analysed to explore the judicial interpretation of privacy and cyber offences. Secondary sources such as books, scholarly articles, NCRB reports, and international conventions like CEDAW and the Budapest Convention on Cybercrime are also consulted to provide a comparative and global perspective. The response of questionnaire and interviews plays an important role in analysing the current legal system for protection of women privacy in the digital era. The methodology involves an analytical approach to assess the effectiveness

[25]Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

[26]Shreya Singhal v. Union of India AIR 2015 SC 1523

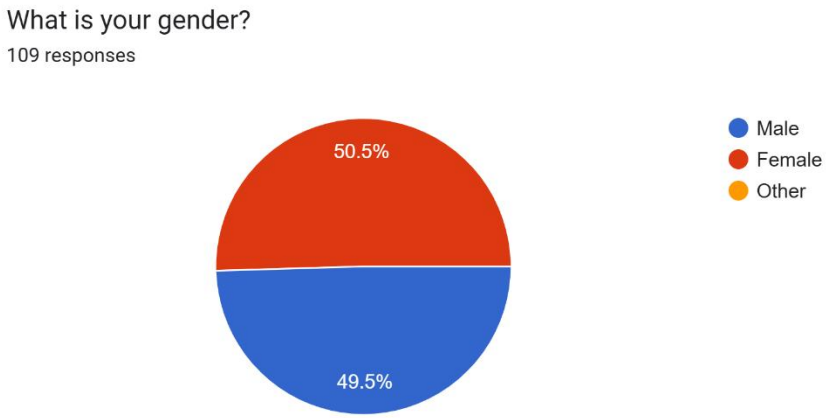
of existing legal provisions in addressing issues of revenge porn, blackmailing, and cyber harassment against women. A comparative dimension is also adopted to identify best practices from other jurisdictions. The ultimate aim of the methodology is to critically evaluate the adequacy of Indian laws, highlight existing gaps, and suggest reforms for better protection of women's privacy in the internet era.

**Challenges in controlling these crime**

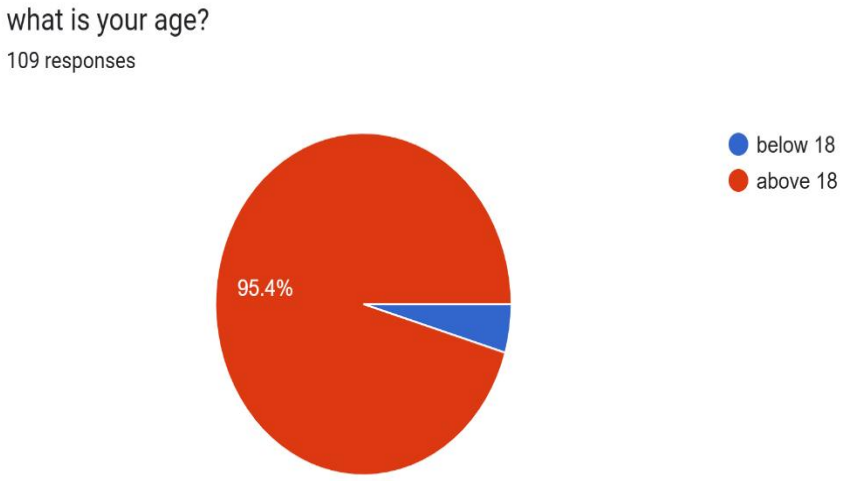
The major challenges in controlling this type of cybercrime like online harassment are: -

- Underreporting crime by women due to fear of social stigma.
- **Jurisdictional issues** in cross-border online crimes.
- **Lack of awareness** among women about cyber laws.
- **Technological anonymity** of perpetrators.

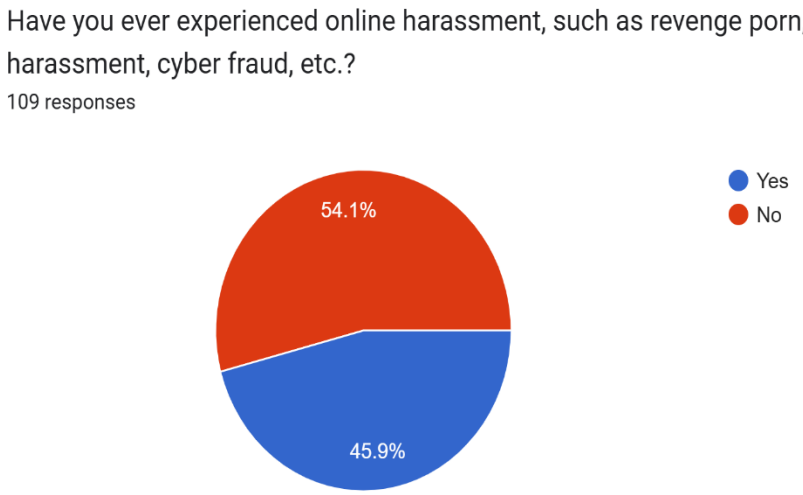
**Research findings:- : -**




This questionnaire is been filled by total 110 different individuals out of which 50.5% of males and 49.5 percent of the females.

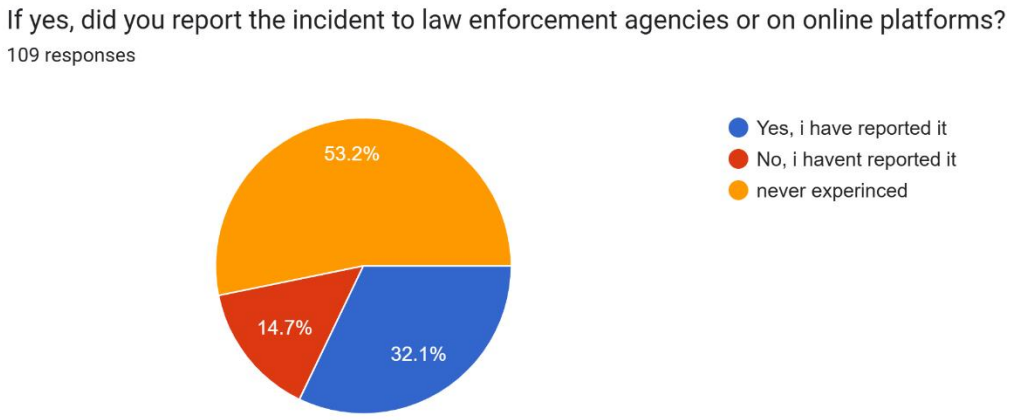



The questionnaire is been filled by 95.4% individuals who are above 18 years of age whereas only 4.6% of individuals are of age below 18 years.

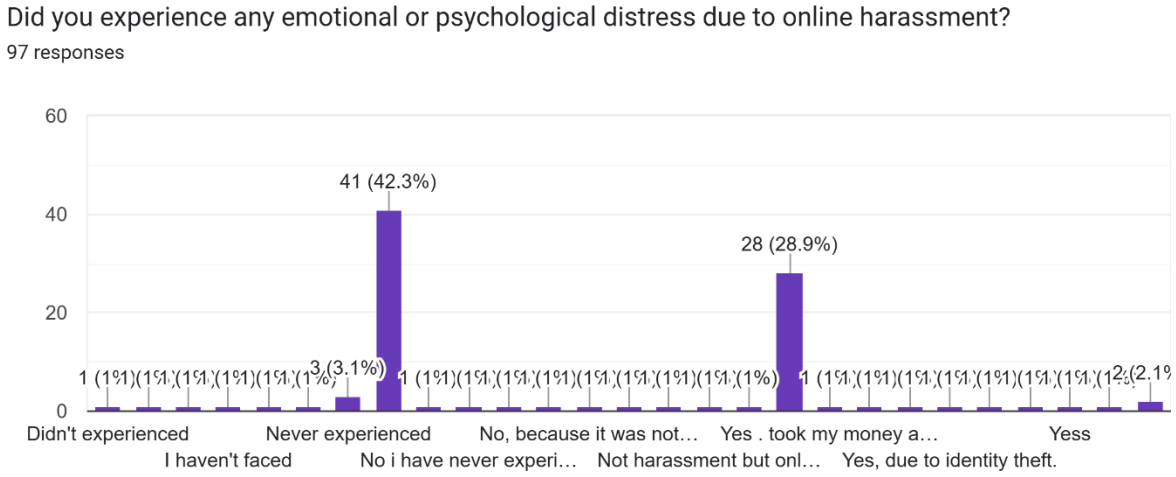



On the question of have you ever experienced online harassment, such as revenge porn, blackmailing, or cyber harassment, cyber fraud, etc. it is find that 54.1% of individuals have never experienced online harassment such as revenge porn where as 45.9% of individuals have experienced revenge porn.

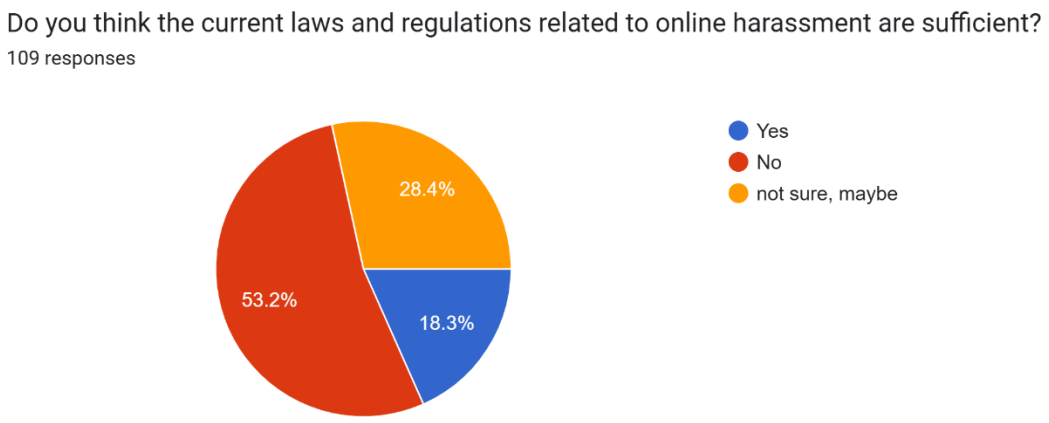
On the question of did they report the incident to law enforcement agencies or on online platforms, it is find out that 32.1% of individuals are those who reported the incident, 14.7%




percent individual never reported any such incident whereas 53.2% of individuals are those who never experienced such crimes.




On question of Did you experience any emotional or psychological distress due to online harassment, it is find out that more that 41% of individual never experienced any emotional or psychological distress due to online harassment whereas more than 50% of individuals are those who face this distress due to different type of online harassment and also there are 7% of individuals who face such emotional and psychological distress due to online trolling to some other person.




On the question of the current laws and regulations related to online harassment are sufficient or not, it is find out that 18.3% individuals' belief that the current laws related to such crime are sufficient whereas 53.2% individuals' belief that the current laws are not sufficient to regulate the online harassment happening in the current time. There are also 28.4% of people who are even not sure about either the current laws are sufficient to regulate or not.

**On the question that What changes would you like to see in the legal framework to better protect women from online harassment?**

The responses of individuals reflect that More than 80% of individuals strongly concern regarding the increasing cases of online harassment against women and the inadequacy of the current legal and enforcement mechanisms in addressing such offenses. Many respondents believe that implementing stricter laws and establishing effective reporting mechanisms is essential to ensure better protection for women in digital spaces. There is a shared opinion that although India has legal provisions under the Information Technology Act, 2000, and other related laws, their implementation remains weak and ineffective. One respondent shared a personal experience of filing a complaint on the cybercrime website, where the account of the offender was blocked and an investigation was initiated, yet no serious action was taken, and the case was later closed due to the inability to trace the accused. This experience highlights a lack of seriousness and efficiency in handling such cases.

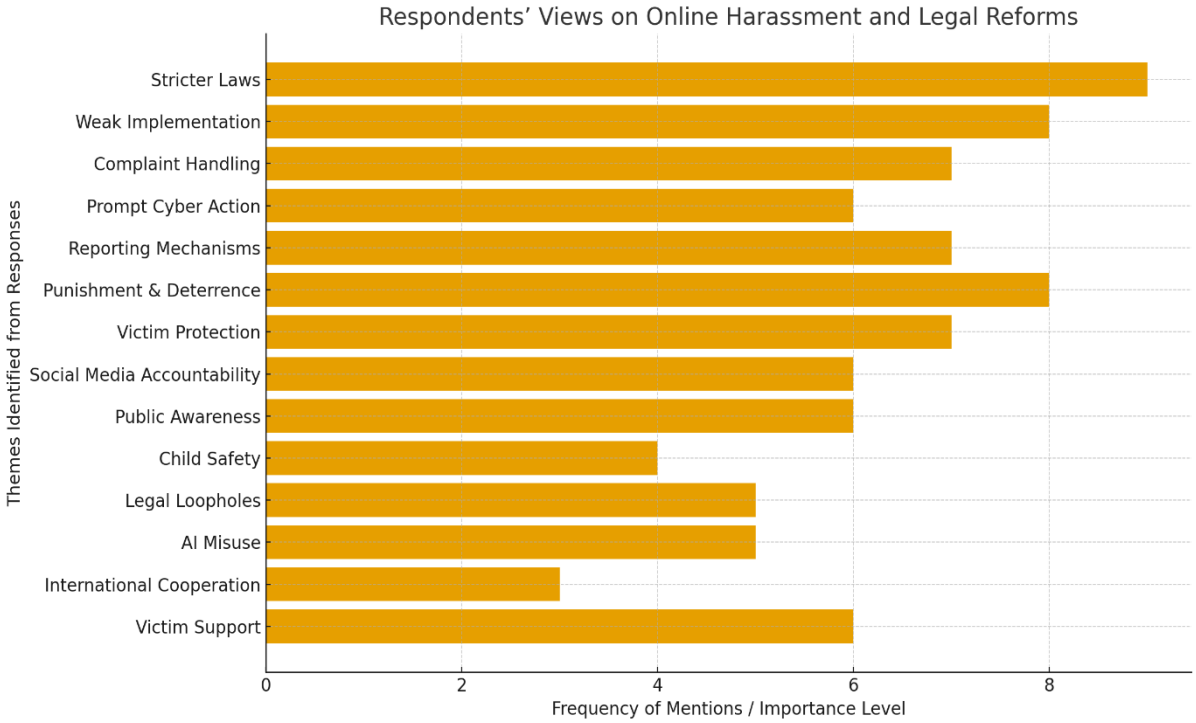
Several individuals expressed that the existing laws are sufficient in theory, but their application and enforcement are inadequate to prevent cybercrimes effectively. Respondents stressed the need for cyber experts and investigating officers to act more promptly and for the introduction of stricter laws and stronger implementation mechanisms. Many emphasized the necessity of inserting strict punishments within the legal framework to create a deterrent effect and ensure that offenders think twice before committing such crimes.

Respondents further suggested that the legal framework should be restructured to include simplified and faster reporting mechanisms, stricter penalties for repeat offenders, and stronger enforcement of cyber laws. It was also recommended that reforms should focus on

safeguarding the identity of victims, ensuring accountability of social media platforms, promoting awareness of digital rights, and strengthening international cooperation in combating cybercrimes. The participants felt that identity verification regulations should be made more stringent, as online harassment often occurs due to the anonymity enjoyed by offenders.

A recurring suggestion was to increase public awareness of cyber laws and ensure that victims receive swift action and justice. Many believed that timely justice would discourage future offenders. According to some participants, every mistake or offense should be punished appropriately so that people are deterred from engaging in online abuse. There was also a strong recommendation for the protection of minor children from the harmful influence of online platforms through specific laws or guidelines addressing child safety in cyberspace.

Respondents identified numerous loopholes in existing cyber laws, such as the absence of a clear definition of "digital harassment." They argued that the lack of a proper definition hampers the development of effective laws and called for the creation of a comprehensive personal privacy law in India. The participants advocated for a victim-centric approach, ensuring that victims' rights, privacy, and well-being are prioritized throughout the legal process. Furthermore, it was suggested that the law should criminalize the unauthorized capture, publication, or transmission of private images without consent and regulate the misuse of artificial intelligence, as AI-generated fake or morphed images are becoming a new form of online abuse. Lastly, respondents recommended establishing a dedicated helpline, stringent imprisonment provisions, and psychological support systems to help victims recover and seek justice more effectively. The major responses given by the individuals are as follows: -

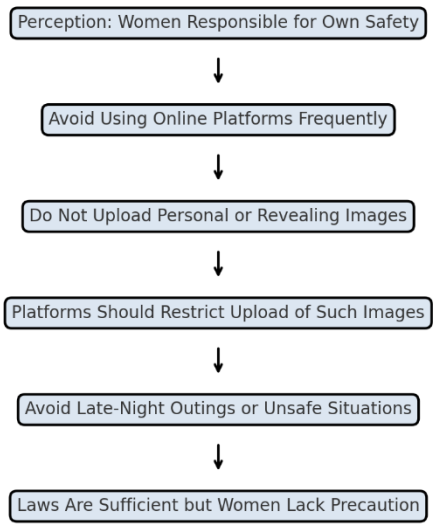


On the same questions there are approx. 20% of individuals responses reflect a viewpoint that emphasizes women's responsibility for ensuring their own safety, both online and offline. Several individuals suggested that girls should limit their use of online platforms, as they are often unsafe and prone to misuse. According to these respondents, women should avoid uploading personal or revealing photographs on social media, as such content may be exploited by others. Some even proposed that websites should restrict or make it difficult to upload such images, thereby reducing the risk of online harassment.

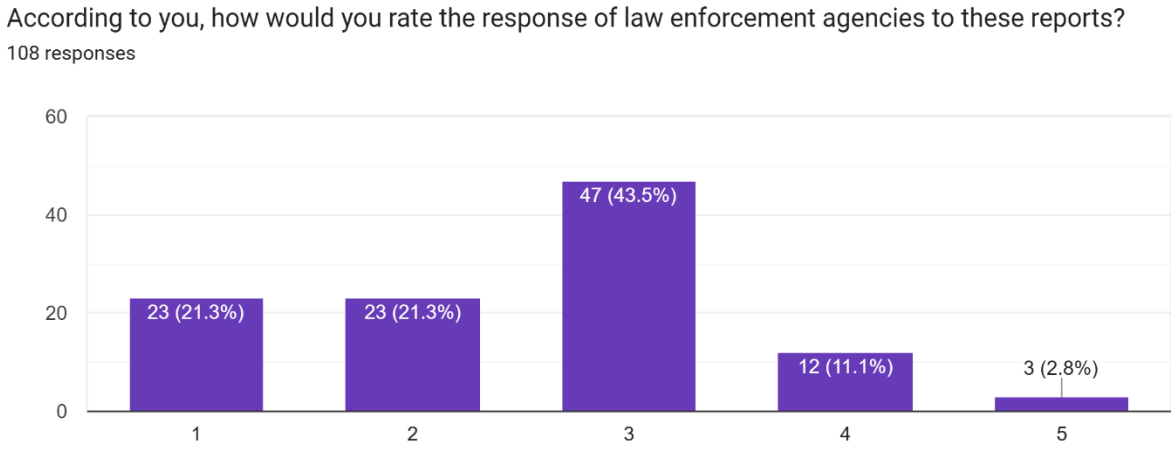
A few participants further stated that wearing short dresses and roaming late at night could make women more vulnerable to harassment, advising greater self-restraint and caution in such situations. They argued that while existing laws are sufficient, women often fail to take necessary precautions to protect themselves in digital environments.

Overall, these responses represent a preventive and conservative outlook, focusing on modifying women's behaviour rather than strengthening systemic protections or enforcing offender accountability. The respondents' views suggest a belief that individual responsibility and cautious conduct are central to preventing online harassment, reflecting a mindset where safety is seen as a personal duty rather than solely a legal or societal obligation.

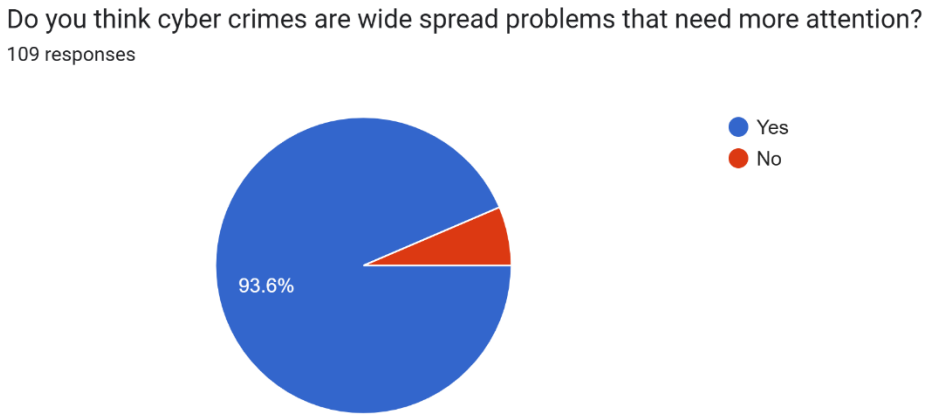
**Flow Chart: Summary of Respondent Views on Women's Online Safety**



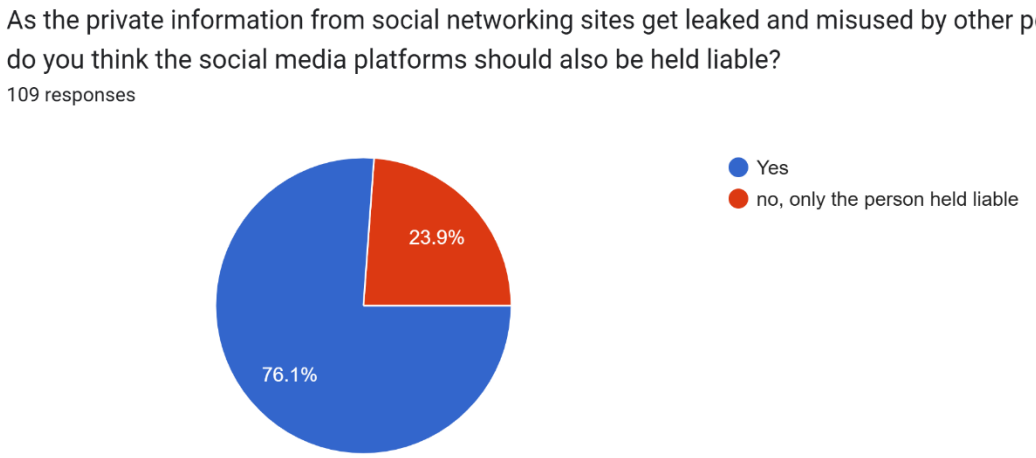

This chart shows the summary of the view of different individuals.



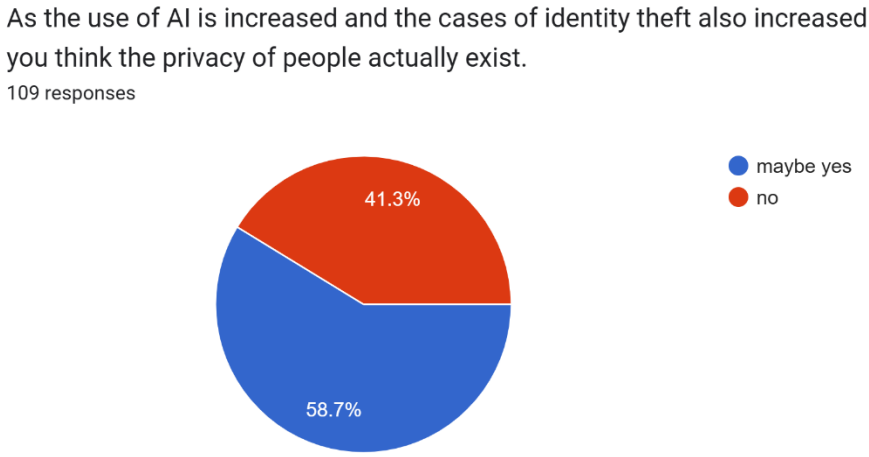

On the question to rate the responses of law enforcement agencies to these complaints out of 5 where 1 is considered as not at all responsive and 5 is considered as very responsive, it is find out that 47 individuals believe that the response of agencies are moderate, 23 individuals believes that the agencies are not at all responsive whereas only 3 individuals believes that these agencies are very responsive to tackle such crime.




On the question that is there need to give more attention to the cyber crime or not, it is find out that 93.6% of individuals believe that there is need to provide more attention on such crimes whereas 6.4% of individuals believes that there is no need to give more attention to such crimes as the existing las are sufficient to control such crime.




On this particular question, it is find out that 76.1% of individuals believes that social media platforms should also be made liable for the leaked information and their misuse by other people whereas 23.9% individuals believes that only the person should be held liable and not the social media platform.




On this question that do privacy of people actually exist in the current time or not, it is find out that 41.3% of individuals believe that privacy does not exist in the current time whereas 58.7% individuals are not sure about whether the privacy exists or not.

**On the question that According to you is there any need for legal framework for new emerged crimes like revenge porn?**

The responses collectively emphasize a strong and unanimous agreement on the urgent need for a comprehensive and specific legal framework to address the growing issue of revenge pornography and related digital crimes. Most respondents expressed concern about the increasing number of cases involving teenagers, highlighting that younger individuals are particularly vulnerable to online exploitation, blackmail, and privacy violations. This rise in

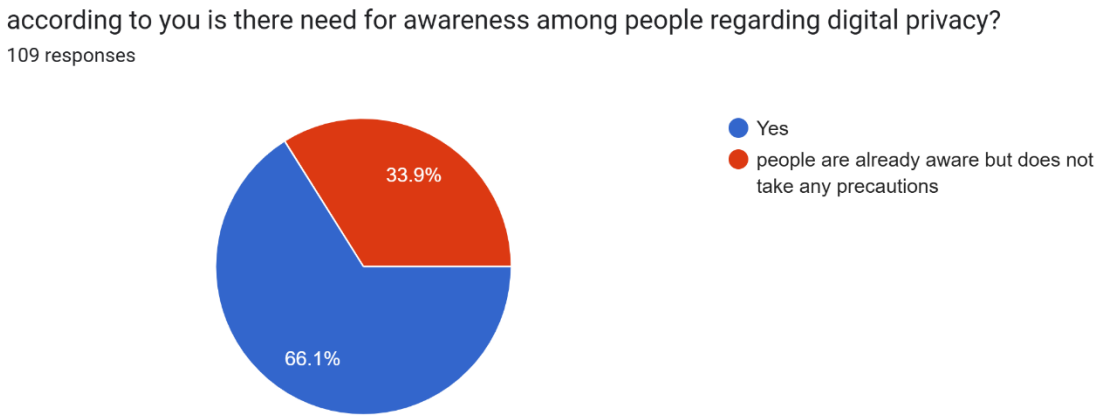
incidents demonstrates how technological misuse has evolved beyond the scope of existing legal mechanisms.

Respondents consistently agreed that there should be a proper, well-organized, and specialized system for handling crimes related to pornography, particularly those involving non-consensual image sharing and deepfakes. They observed that the current laws in India, such as the Information Technology Act, 2000, and provisions under the Indian Penal Code, do not adequately address the complexities of newly emerging forms of digital abuse. Many participants argued that existing laws are too broad, outdated, and lack clear definitions for crimes like revenge porn, image-based sexual abuse, and digitally altered content.

A recurring theme across the responses was the need to protect personal dignity and privacy, especially for women and minors who are disproportionately affected by such offenses. Respondents emphasized that crimes involving intimate images or videos violate an individual's right to privacy, bodily autonomy, and human dignity. They asserted that a modern, victim-oriented legal system must ensure quick investigation, strict punishment for offenders, and confidentiality for victims throughout the legal process.

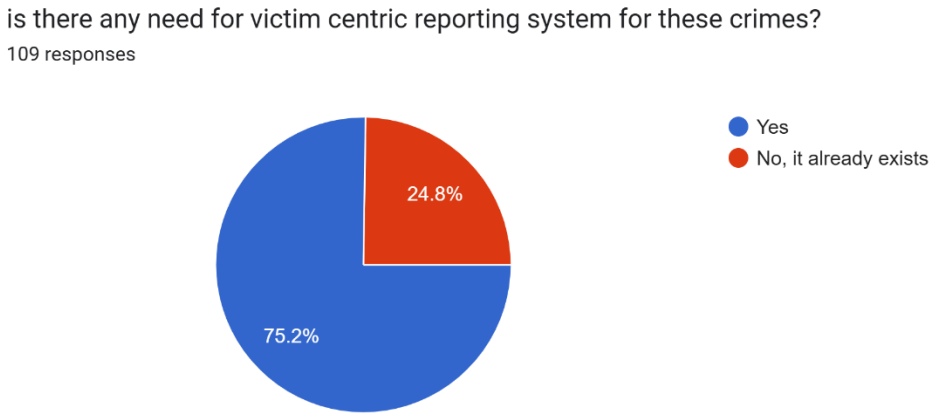
Furthermore, participants pointed out that as technology advances rapidly, new forms of abuse such as deepfakes and AI-generated explicit content have emerged, making it even more crucial to have specific, up-to-date legal provisions. They believed that clearer laws would help ensure faster action, stronger penalties, and better protection for victims, while also deterring potential offenders.

Some respondents also linked the growing digital misuse to psychological and moral concerns, noting that uncontrolled access to explicit content contributes to an increase in such crimes. They emphasized that a well-defined legal structure, supported by awareness programs and ethical regulation of digital content, is necessary to safeguard public morality and ensure responsible behaviour online.




On the question that there is need for awareness among people regarding digital privacy, it is find out that 66.1% of individuals believes the need for awareness among people regarding

digital privacy whereas 33.9% of individual believes that people are already aware but does not take proper precautions.




On the question that is their need for victim centric reporting system for these crimes, it is find out that 75.2% of individuals believes that there is need of victim centric reporting system whereas 24.8% of individuals believes that the victim centric reports already exist.

**On the question that why do you think major crimes related to women remain unreported as well as unnoticed?**

The responses reveal a deeply rooted social and psychological dimension behind the underreporting of cybercrimes and other crimes against women. A clear pattern emerges from the views shared — that the fear of social stigma, societal pressure, and lack of trust in law enforcement are the most significant factors discouraging women from reporting online harassment or sexual exploitation. Many respondents emphasized that women, especially in traditional and conservative societies, refrain from seeking justice due to the fear of being blamed, shamed, or ostracized by their own families and communities.

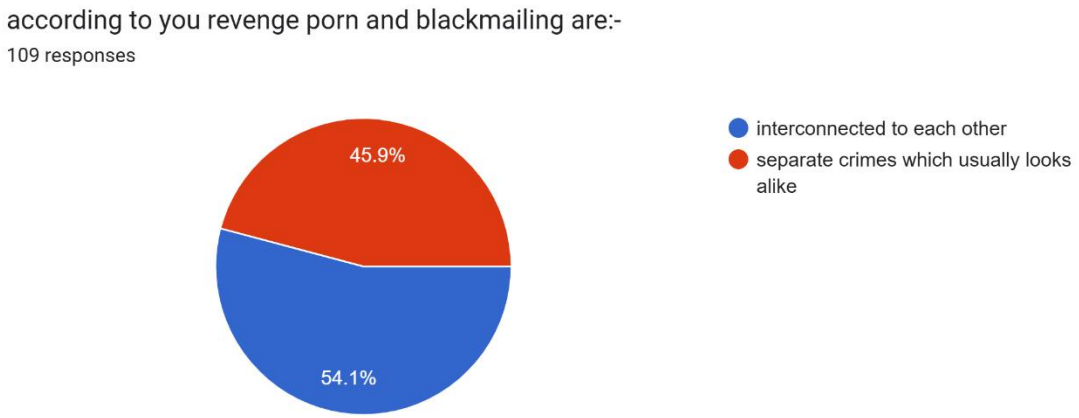
A recurring theme is the societal perception of women's dignity. Respondents repeatedly mentioned that women fear reporting incidents because they worry about losing respect within their families and neighbourhoods. Crimes like revenge porn or online abuse are often associated with notions of "character" and "honor," and many victims fear being judged rather than supported. This honor-based mindset creates a culture of silence, where protecting family reputation becomes more important than seeking justice. Respondents noted that families themselves often discourage victims from filing complaints to "avoid bringing shame" upon the household.

Several participants highlighted that lack of awareness among women and girls regarding cyber laws and reporting mechanisms adds to the problem. Many victims are unaware of how or where to report cybercrimes, and even when they attempt to do so, law enforcement authorities are often perceived as dismissive or unhelpful. This lack of institutional sensitivity and support further reinforces women's reluctance to come forward. Respondents expressed that the

authorities often take cybercrimes less seriously, viewing them as minor or non-physical offenses, which results in victims feeling that justice will not be served.

Another significant reason identified in the responses is the absence of family and community support. Many women lack the courage to report crimes because they anticipate judgment, criticism, or disbelief from their own relatives. The emotional and psychological burden of potential social consequences, combined with the lengthy and often intimidating legal process, leads victims to remain silent. Fear of retaliation or further harm from the offender also contributes to this hesitation.

Respondents also pointed out that the slow pace of the judicial process and lack of immediate action discourage victims from pursuing complaints. As a result, many cases go unnoticed, allowing perpetrators to act with impunity. This cycle of silence, fear, and institutional failure contributes to the weakening of women's safety and dignity in society.




On the particular question it is find out that 54.1% of individuals believe that revenge porn and blackmailing are interconnected to each other whereas 45.9% of people believes that both revenge porn and blackmailing are separate crimes which looks alike.

**Analysis and discussion:**

The research findings reveal a significant prevalence of online harassment and privacy violations targeting women in the digital space. Among 110 respondents, 54.1% reported experiencing cyber harassment, including revenge porn, blackmailing, and other forms of online abuse. Over half of these victims reported emotional and psychological distress, highlighting the profound impact of such crimes on women's mental health and overall well-being. These results indicate that online harassment is not only a legal issue but also a pressing social and psychological concern that requires multifaceted intervention.

The study identifies a notable gap between the legal provisions in place and their effective implementation. Only 18.3% of respondents believe that existing laws sufficiently protect

women, while more than half consider them inadequate. Respondents highlighted systemic inefficiencies, such as delayed investigations, lack of accountability, and insufficient action by law enforcement agencies, as significant barriers to justice. Experiences shared in the study, such as complaints on cybercrime portals resulting only in blocked accounts without further action, reflect procedural weaknesses that undermine the protective intent of current laws.

A major theme emerging from the responses is the urgent need for a **victim-centric legal framework**. Participants emphasized stricter laws, faster and simplified reporting mechanisms, protection of victim identities, harsher penalties for repeat offenders, and accountability of social media platforms. The study also underscores the necessity of updating legal provisions to address emerging forms of abuse, including AI-generated content and deepfakes, which are not adequately covered under current legislation.

Social and cultural factors further contribute to the underreporting of online harassment. Fear of social stigma, societal pressure, and potential damage to family "honor" discourage victims from filing complaints. The findings reveal that awareness of digital rights is limited, and trust in law enforcement is low, which exacerbates women's vulnerability online.

Findings reveals that there are people who believe that laws are lacking due to which the privacy of women are at risk. And there is need to implement the laws strictly. The perspective of both men and women differs from each other which is mentioned as follows: -

| **S.no.** | **Questions** | **In male point of view** | **In female point of view** |
|---|---|---|---|
| **1.** | **Why revenge pornography occurs.** | For blackmailing for the financial needs or any other benefit. | For revenge purposes of the sufferings by any manner. |
| **2.** | **Do women are really the victim.** | Sometimes | Always |
| **3.** | **Solution to reduce the rate of revenge pornography.** | Make new laws protecting the privacy of both male and female and does not focus only on the female protection laws. | 1. Avoid the sharing of the intimate pictures with anyone.<br>2. Gender equality laws should be more accurate. |
| **4.** | **privacy of men is more important or women.** | Both | Both |

## Conclusion

While India has developed a **robust legal framework** combining the IT Act, IPC, and constitutional guarantees, the evolving nature of technology requires continuous legal adaptation. Women's privacy in the internet era must be protected not only through laws but also via social awareness, digital literacy, and effective enforcement. According to some scholars, revenge porn, is the online publication of sexually explicit images or films without the consent or knowledge of the subject. here blackmailing and Revenge pornography can be considered as inter related to each other. This research paper focuses on how private data get leaked and be selled on the dark web ([27]Kalpana bhandari vs sebi 2003 case).

In conclusion, the research emphasizes that safeguarding women's digital privacy demands an integrated approach combining robust legal reform, effective enforcement, public awareness, and technological regulation. A specialized and victim-oriented framework is essential to ensure timely justice, protect privacy, and deter offenders, thereby creating a safer and more equitable digital environment for women.

This research paper focus on different perspective of people about cyber crime and protection of women. This research paper helps a lot to understand that the crime rate is increasing with the developing technology, and the mentality of people also narrows down. People of new generation still have that orthodox thinking. People of present generation still objectify the women due to their gender and their clothes. After doing deep research, it is not wrong to say that only the technology is advancing but not the mindset of people. Not only the legal framework and provisions are lacking in the current time but also the public awareness, institutional accountability, and social support systems is lacking.

The people want the legal provisions to be stricter and more strict punishment to be given to the offender so that it will give a deterrent effect in mind of other people but for this, the mindset of people is needed to be changed. It can be seen as people wants the society to be changed but they don't want to take any initiatives from themselves to change the society.

## Suggestions and Recommendation

- Stronger data protection laws (pending **Digital Personal Data Protection Act, 2023**).
- Creation of specialized cyber cells and fast-track courts.
- Awareness campaigns for digital literacy and women's cyber safety.
- Mandatory due diligence for social media platforms to curb revenge porn.

[27] Kalpana Bhandari And Ors. vs Securities And Exchange Board Of India ... on 5 August, 2003 Equivalent citations: 2004(1)BOMCR663, [2005]125COMPCAS804(BOM)

**Scope for future research**

- Analysis of effectiveness of legal provisions and enforcement mechanism.
- The role and responsibility of social media platform in case of privacy breach.
- Analysis on the victim centric approach made by the legislation is sufficient or not.

**REFRENCE: -**


1. Smith, A. (2016). *Revenge pornography* [Dissertation].
2. Khatri, K. (n.d.). *Article 20*. *Observer Research Foundation (ORF Online)*. Retrieved from https://www.orfonline.org
3. Wikipedia contributors. (n.d.). *Revenge porn*. *Wikipedia*. Retrieved November 4, 2025, from https://en.wikipedia.org/wiki/Revenge_porn
4. Nyaaya. (n.d.). *Is revenge porn a crime in India? Nyaaya Weekly*. Retrieved November 4, 2025, from https://nyaaya.org/nyaaya-weekly/is-revenge-porn-a-crime-in-india/#:~:text=Yes.,the%20Information%20Technology%20Act%2C%202000
5. *Cyber law.* (n.d.). *National Centre for Internet and Broadband (NCIB)*. Retrieved from https://www.ncib.in/pdf/cyber-law.pdf
6. Goyal, S. (2022). *Cyber crimes against women and prevention*. *International Journal of Multidisciplinary Educational Research*, *III*(2), 98–108.
7. *Cyberra Legal Services.* (n.d.). *Case studies on cyber law*. Retrieved from https://www.cyberralegalservices.com/detail-casestudies.php