

A CRITICAL STUDY OF CYBER OFFENCES AGAINST WOMEN AND THE ROLE OF LAW: WITH SPECIAL REFERENCE TO PRESIDENCY UNIVERSITY, BENGALURU

¹Dr. Neha Gupta, ²Ms. Soyonika Gogoi

¹Assistant Professor, School of Law, Presidency University, Itgalpur, Rajanukunte, Yelahanka, Bengaluru-560064 (Karnataka State), India, Email: neha1007gupta@gmail.com

²Assistant Professor, School of Law, Presidency University, Itgalpur, Rajanukunte, Yelahanka, Bengaluru-560064 (Karnataka State), India, Email: soyonika.gogoi@presidencyuniversity.in

ABSTRACT

The internet has revolutionised how people connect, work, and express themselves, but for many women it has also introduced new dimensions of vulnerability. Digital platforms, while enabling empowerment, have simultaneously exposed women to a spectrum of cyber offences such as online abuse, impersonation, cyber stalking, doxxing, cyber pornography, cyber harassment, trolling, etc. These online harms often mirror and exacerbate real-world gender inequalities, making digital spaces increasingly unsafe.

This paper aims to critically explore the growing pattern of cyber offences targeted at women and evaluate the strength and shortcomings of current legal responses. It analyses whether women are aware about various cyber-crimes and the redressal mechanism available to them. The paper also investigates whether existing legal instruments are equipped to address the unique nature of online gender-based violence, and how they can be improved to ensure timely justice and effective prevention. Using empirical and doctrinal research approach, researchers examine the types of cybercrimes against women and the remedy available to the victims. The paper also examines key provisions in Indian cyber law, particularly the Information Technology Act, 2000, along with allied criminal laws and considers comparative international practices and multilateral efforts to combat cybercrime. The analysis is supported by judicial interpretations, government reports and recent developments in digital policy.

The research finds that while legal systems are evolving, they often lag behind the fast-changing digital environment. Victims, especially women, face challenges related to reporting cybercrimes, accessing legal remedies and receiving timely institutional support. The lack of gender sensitivity and digital awareness among enforcement agencies further limits the impact of current laws. The paper advocates for more inclusive, tech-responsive and survivor-friendly legal frameworks, as well as improved digital literacy and international collaboration to make online spaces truly safe for women.

KEYWORDS: Cybercrime, Cyber Law, Digital Violence, Gender Justice, Online Harassment, Women's Rights

1. INTRODUCTION

Globalization has played a key role in shaping modern communication systems, with the Internet standing out as one of the most influential developments. With the growth of rapid technological advancements, the Internet has allowed people and businesses to connect, communicate and operate across borders like never before. It has essentially turned the world into a global village, where information flows freely and instantly and opportunities for collaboration are endless. New digital tools and communication technologies have changed not just how we live, but how we work, interact and manage everyday tasks. Replacing standard paper documents, we now create, send and store information electronically because it is speedier, efficient and easier to access.

However, alongside these innovations comes a dark reality. The same technology that connects us has also opened doors to anonymous activity in cyberspace, leading to a surge in cybercrimes. As digital spaces become increasingly embedded in our daily lives including online businesses and remote jobs to advocacy, political campaigning and social networking, cyber threats have also grown in scale and sophistication. Unfortunately, online platforms can often be hostile environments. Individuals who voice unpopular opinions or challenge it may find themselves silenced, harassed, or even excluded through various forms of cyber abuse. (Pathak & Tripathi) This not only stifles freedom of expression but highlights the urgent need to build safer, more inclusive digital spaces. While the Internet continues to offer incredible possibilities, it also demands thoughtful regulation and collective responsibility to ensure it remains a force for good.

Cybercrime refers to the act of unlawfully creating, distributing, modifying, stealing, abusing, or damaging information via computer systems, carried out without physical force and without the consent of the victim. (Padmavathi, 2015). As per the National Crime Records Bureau (NCRB) 2022, a total of 65,893 cybercrime cases were reported in 2022, reflecting a 24.4% increase compared to the 52,974 cases registered in 2021. Correspondingly, the cybercrime rate rose from 3.9 per 100,000 population in 2021 to 4.8 in 2022. Among the reported cases in 2022, fraud constituted the

majority motive, accounting for 64.8% (42,710 cases), followed by extortion at 5.5% (3,648 cases) and sexual exploitation at 5.2% (3,434 cases). (National Crime Records Bureau, 2022)

Cybercrimes affect both men and women alike, with individuals of all genders falling victim to perpetrators who seek to exploit them unjustly. While digital victimization is not a new phenomenon, its significance has increased in recent times, particularly following the introduction of legal provisions aimed at penalizing cyber offences. The current state of cyber security in India is a cause of concern as women are more vulnerable to such cyber crimes. Safety of women has long been a matter of concern, particularly in a country like India, where crimes against women continue to rise at an alarming rate. Traditionally, such threats were largely confined to public spaces such as streets or remote areas. The home, once considered a refuge and the safest place for women, is increasingly becoming a site of vulnerability. Recent trends indicate that domestic environments are no longer immune to gender-based violence and exploitation, highlighting the pervasive and evolving nature of threats to women's safety. (Goyal, 2022) Cybercrime poses serious consequences for women in India, which is significantly impacting both their mental and emotional well-being. The rapid expansion of social media and digital platforms has led to a high rise in cases including cyber bullying and online harassment, with women disproportionately targeted. Forms of cyber threats such as cyber stalking, identity theft, and non-consensual sharing of intimate content, commonly referred to as revenge pornography have become alarmingly prevalent. These acts often result in profound psychological distress, emotional trauma, and long-term mental health issues for the victims. Moreover, cybercrime has exerted a substantial economic impact on women, with many experiencing job loss or financial setbacks as a result of online fraud and related cyber offences. (Yadav, 2022)

1.1 Overview of cybercrimes against women

Women during the ancient years were given a place at a higher pedestal who was at par to that of great monarchs and deities who held significant positions in society. However, despite having vital roles in society, they are among the most vulnerable groups and are open subjected to violation of every sort. Violence against women not only includes physical violence but also includes emotional, sexual, psychological and financial abuse. A very common kind of abuse in the present times is the violence faced by women in the digital space. In a study conducted by the United Nations Economic and Social Commission of Asia and the Pacific (ESCAP), it shows that there is a significant digital divide between the male and female populations worldwide as a result of an increase in sexual cybercrimes against women.

Region / Continent	Men (%)	Women (%)
2020 Report (General)	58.3	48.4
Asia (2020)	54.6	41.3

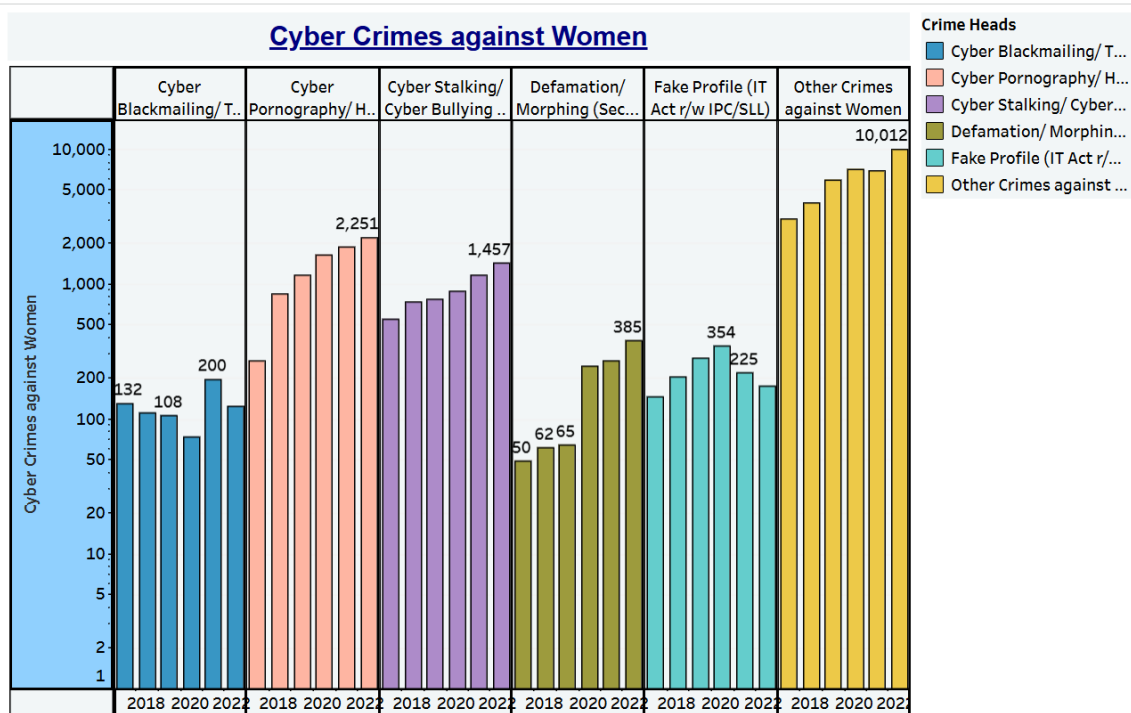
The table shows the gender-wise use of internet services in 2020. At the global level, 58.3% of men and 48.4% of women accessed the internet. In Asia, the gap is wider, with 54.6% of men using internet services compared to only 41.3% of women. This highlights a noticeable digital gender divide both globally and regionally. (ESCAP, 2021)

In India, where cybercrimes against women have surged in recent years; women have been disproportionately impacted by such crimes. Women have been severely victimized in cyberspace and their mental and physical health suffers as a result of cybercrime. With the rise of social media and online platforms, cyber bullying and online harassment which primarily target women have become a concern. There are multiple cybercrimes committed against women such as misuse of digital platforms to harass, threaten or exploit them. These crimes often target their privacy, dignity and emotional well-being. The increasing use of social media, messaging apps, and online platforms has made women more vulnerable to such offences. According to the latest NCRB report 2022, cyber crimes against women have increased by 11% compared to the 2021 data. (National Crime Records Bureau, 2022).

In our country, women are mostly victims of cybercrimes such as revenge pornography, cyber bullying, cyber stalking and cyber harassment. Cyber bullying is the use of technology to harass, degrade or threaten someone whereas online harassment consists of sending threatening or insulting messages or remarks on social media sites. A pattern of recurrent online harassment that includes tracking, watching or following someone's online activities is known as online stalking. The spread of sexually explicit photographs or films without the victim's agreement is known as revenge pornography, while online financial frauds such as credit card fraud and phishing are examples of cyber financial fraud. Women have become increasingly susceptible to cybercrime due to the exposure of their personal information. There is a clear link between female victimization and the rise in cybercrimes, with each often contributing to the other. (Dutta, 2023)

1.2 Kinds of Cyber crimes against women

As per a study conducted by the National Crime Records Bureau, the cyber crimes such as Cyber blackmailing or threatening, Cyber pornography, cyber stalking, defamation or morphing, creation of fake profile and other crimes committed against women have increased to a great extent between 2018 and 2022.



Source: Ministry of Statistics and Programme Implementation

The data highlights a steady rise in cybercrimes against women in India between 2018 and 2022 across six categories. Cyber pornography/harassment shows the sharpest increase, crossing 2,250 cases by 2022, while cyber stalking/bullying nearly doubled to 1,457 cases. Fake profile cases peaked in 2020 but persist, and defamation/morphing incidents continue to grow gradually. The “Other Crimes” category remains the largest, surpassing 10,000 cases in 2022. Overall, the trend reflects women’s increasing vulnerability online and the urgent need for stronger laws, digital literacy, safeguards, and gender-sensitive cyber policing.

1.3 Nature and types of cybercrimes against women

Cybercrimes targeting women include a wide array of offenses:

1. Cyberstalking
2. Email harassment
3. Cyber defamation and trolling
4. Image morphing and identity theft

Major Cyber crimes are as under:

1. Cyber Bullying and Flaming: A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc. sexual act. Flaming is a form of cyber bullying where offensive or hostile messages are sent directly to the target through texts, emails, or online platforms. Such communication often includes abusive, vulgar, and aggressive language intended to provoke or hurt the victim.
2. Cyber Stalking: Cyber stalking is on the rise and women are the most likely targets. Cyberstalking is a way to use the Internet to stalk someone for online harassment and online abuse. A cyber stalker does not engage in direct physical threat to a victim but follows the victim's online activity to gather information, make threats in different forms of verbal intimidation.
3. Harassment through e-mails: Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Harassment includes blackmailing, threatening, bullying, and even cheating via email. E-Harassment is similar to the letter harassment but creates problem quite often when posted from fake ids.
4. Cyber Defamation: Cyber defamation includes both libel and defamation. It involves publishing defamatory information about the person on a website or circulating it among the social and friends circle of victims or organisation which is an easy method to ruin a women's reputation by causing her grievous mental agony and pain.
5. E-Mail Spoofing: it generally refers to an e-mail that emerges from one source but has been sent from another source. It can cause monetary damage.
6. Cyber Phishing: Phishing is the attempt to gain sensitive information such as username and password and intent to gain personal information.
7. Cyber Morphing: Morphing is editing the original picture by unauthorized user or fake identity. it was identified that female's pictures are downloaded by fake users and again re- posted /uploaded on different websites by creating fake profiles after editing it .
8. Cyber Trolling: Trolls spreads conflict on the Internet, criminal’s starts quarrelling or upsetting victim by posting inflammatory or off-topic messages in an online community with the intention to provoke victims into an emotional, upsetting response. Trolls are professional abusers who, by creating and using fake ids on social media, create a cold war atmosphere in the cyber space and are not even easy to trace.

9. Cyber pornography and grooming: Cyber pornography refers to the act of publishing, transmitting or facilitating the communication of material in electronic form that depicts sexually explicit acts or behaviour and Cyber grooming involves the use of the internet to establish a relationship with an individual with the intention of manipulating, exploiting, or coercing them, often for sexually motivated acts. (Muskan, 2025)

10. Cyber Voyeurism: Cyber voyeurism refers to the unauthorized intrusion into an individual's private digital or online spaces often carried out without their knowledge or consent. It involves secretly accessing, observing, or recording someone's personal moments or activities, usually with the intent to exploit, harass, or violate their privacy. This form of cyber offence is particularly harmful as it invades the dignity and security of individuals in the digital environment

11. Doxxing: Doxxing refers to the act of intentionally disclosing or publishing an individual's private or personal information such as home address, phone number, or financial details on public platforms without their consent. This practice is often done with malicious intent to harass, threaten, or endanger the targeted person, making it a serious violation of privacy and security in the digital space.

II. LITERATURE REVIEW

Scholarship on cyber offences against women in India converges on three themes: (i) the gendered nature of access and participation online; (ii) the typology and prevalence of online harms; and (iii) the evolving but fragmented legal-regulatory response. Global policy literature documents a persistent digital gender gap that shapes exposure to risk and the capacity to seek remedies. The World Bank synthesising ITU estimates for 2019 notes that 58.3% of men versus 48.4% of women used the Internet globally, with gaps widening in several regions outside Europe and Central Asia. This unequal baseline of access intersects with socio-cultural factors to produce distinct patterns of harm and under-reporting among women users. (Group, 2021)

Indian empirical sources corroborate both the growth and changing character of cyber offences. The National Crime Records Bureau (NCRB) Crime in India 2022 reports a sharp rise in cybercrime cases overall, with frauds constituting the largest share and sexual exploitation and cyber-stalking/bullying of women representing significant subsets; allied dashboards from the Ministry of Statistics and Programme Implementation (MoSPI) provide state-wise and offence-wise break-ups (including §354D IPC read with IT Act). While definitional and reporting issues persist across States/UTs, the trendline across 2018–2022 reflects consistent growth in complaints of cyber pornography/obscenity, defamation/morphing, and fake profiles, alongside a broader “other offences” bucket signalling under-classification. (GOI, 2025)

Doctrinal writing emphasises that India's legal response sits at the intersection of constitutional guarantees, the Information Technology Act, 2000 (as amended), and general criminal law. At the constitutional level, the Supreme Court's nine-judge decision in Justice K.S. Puttaswamy (2017) located informational privacy and dignity within Article 21, framing the digital sphere as an extension of protected autonomy—an anchor for proportional restrictions and a backdrop to statutory interpretation in cases involving doxxing, non-consensual image sharing, and surveillance. (JUSTICE K.S. PUTTASWAMY VS. UNION OF INDIA, 2017)

Within cyber law, *ShreyaSinghal v. Union of India* (2015), which invalidated §66A IT Act and read down §79 notice-and-takedown, remains a watershed for online speech and intermediary liability. For women victims, the judgment had a dual effect: removing an overbroad speech offence while sharpening the lawful pathways for content removal through court/government orders, thereby requiring victims and law enforcement to navigate more formal takedown mechanisms for abusive content. Subsequent commentary tracks persistent attempts to revive §66A-like enforcement and underscores the practical challenges for survivors seeking swift relief. (*Shreya Singhal v. Union of India*, 2015)

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and their 2022–2023 amendments introduced due-diligence obligations (including appointment of compliance, nodal, and grievance officers for significant social media intermediaries), expedited complaint handling, and Grievance Appellate Committees (GACs) for user appeals. These rules attempt to create faster pathways for removal of non-consensual intimate imagery, deepfakes, impersonation, and other harms disproportionately affecting women, while civil society critiques caution against over-broad takedown standards and risks to free expression. Recent government advisories further call on platforms to combat impersonation and deepfakes, reflecting the fast-evolving risk landscape. (India: Grievance Appellate Committees (GACs), n.d.)

Case law applying general and cyber-specific offences to gendered harms is gradually accumulating. A frequently cited early conviction is *State of West Bengal v. AnimeshBoxi* (2018), where a trial court imposed imprisonment for non-consensual dissemination of intimate images, using a combination of IPC provisions (§§354A/354C/354D/509) and IT Act §§66C, 66E, 67, 67A. The case illustrates prosecutorial reliance on a mosaic of offences to address conduct now commonly described as “revenge pornography,” and it foregrounds evidentiary and jurisdictional issues typical of platform-mediated crimes. (CYRILLA, n.d.)

The criminal-law baseline itself is in transition. With the *Bharatiya Nyaya Sanhita, 2023* (BNS) replacing the IPC from July 2024, several offences historically used in cyber-violence cases against women (e.g., stalking, voyeurism, outraging modesty) have new section numbers and, in some instances, updated text. Contemporary practice literature notes that, in tandem with IT Act provisions (e.g., §§66C/66D identity and cheating by personation; §66E privacy; §§67/67A/67B obscenity and sexually explicit material), prosecutors now plead the BNS counterparts for gendered offences, requiring careful citation updates in scholarly and policy work. (Affairs)

Comparative and policy studies agencies, development banks, and newsroom/NGO reports converge on two practical gaps: low digital literacy/awareness among potential complainants and limited gender-sensitive capacity within enforcement. Programmatic responses include specialised cyber support centres and helplines offering legal-technical-

psychological assistance to victims of cyber-harassment and image-based abuse; early evaluations suggest improved reporting but uneven redress. (India, 2025)

Overall, the literature depicts a system mid-stream: rights-protective constitutional doctrine, expanding intermediary obligations, and a refreshed penal code provide scaffolding, but timeliness of takedown, cross-platform cooperation, and survivor-centric procedures remain primary bottlenecks. The empirical signalising complaints and diversification of offence typesunderscores the need for clearer standard operating procedures for platforms and police, better digital evidence handling, and swift civil-criminal remedies tailored to women's experiences online.

3. Research Problem

Despite the rapid expansion of internet use and the proliferation of digital platforms, women in India remain disproportionately vulnerable to cyber offences such as cyberstalking, impersonation, non-consensual dissemination of intimate images, and online harassment. The Information Technology Act, 2000, in conjunction with provisions of the Indian Penal Code (now replaced by the Bharatiya Nyaya Sanhita, 2023), provides certain remedies. However, these frameworks were not originally designed to address the gendered and technologically complex nature of cyber offences. Judicial interventions, such as *ShreyaSinghal v. Union of India* and *State of West Bengal v. Animesh Boxi*, have filled some gaps but have also revealed inconsistencies in enforcement and protection.

Victims frequently encounter obstacles in reporting offences, securing timely takedown of objectionable content, and obtaining survivor-centric support from enforcement agencies. Compounding these challenges are the low levels of digital literacy, gender-insensitive policing practices, and limited awareness of redressal mechanisms. The core research problem, therefore, lies in evaluating whether the existing legal framework in India is adequate to protect women against emerging forms of cybercrime, and in identifying the gaps that necessitate reform, policy innovation, and comparative insights from international best practices.

III. Research Problem

India's escalating cybercrime rates place it among the top five most affected nations globally, reflecting critical gaps in the implementation of cybersecurity measures despite legislative efforts. Limited awareness and inadequate digital literacy among the public and law enforcement further worsen the issue. For women, the threat is particularly severe, as offences such as online harassment, stalking, cyberbullying, non-consensual pornography, and financial fraud not only endanger their mental and physical well-being but also undermine their economic security. The absence of a comprehensive and gender-sensitive approach, combining stronger laws, effective enforcement, public awareness and victim support, continues to hinder meaningful protection against cybercrimes targeting women.

IV. Research Objectives

- 1.To identify and classify different cyber offences relating to women and the legal remedies available.
- 2.To evaluate key provisions in Indian Cyber law, particularly the IT Act, 2000.
- 3.To analyse judicial responses, policy reports and international best practices in order to highlight gaps in the current legal approach to cyber offences against women.
- 4.To suggesta more inclusive, tech-responsive and survivor-friendly legal framework.

V. Research Questions

- 1.In what ways are cyber offences categorised under the Information Technology Act, 2000, along with other relevant legal statutes in India?
- 2.How can advancements in technology be effectively incorporated into law enforcement and judicial processes to enhance responsiveness towards cyber offences targeting women?
- 3.What specific gaps, limitations, and ambiguities exist within the Information Technology Act, 2000, concerning the regulation of cybercrimes?

VI. Hypothesis

H1: The Information Technology Act, 2000 is inadequate to effectively address emerging forms of cyber offences, particularly those targeting women.

H1: Women are less likely to report cyber offences to the appropriate authorities, except in cases involving financial fraud.

H1: There exists a significant lack of awareness among women in Presidency University regarding the different types of cyber offences and the procedures for reporting them.

VII. RESEARCH METHODOLOGY

This study employs a combined doctrinal and empirical approach to analyse the legal framework addressing cyber offences against women in India. The doctrinal aspect involves a detailed examination of laws, judicial decisions, government publications, and academic literature. Key legal instruments considered include the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and provisions covering offences such as cyberstalking, identity theft, voyeurism, publication of obscene material, and online harassment. Landmark judgments, including *Shreya Singhal vs. Union of India* and *State of West Bengal vs. Animesh Boxi*, are analyzed to understand how courts interpret these laws in cases of gender-based online violence.

The empirical component involves primary data collection through a structured questionnaire targeting women aged 18–60 in the School of Law and the School of Engineering at Presidency University, with a total sample of around 1000

respondents. This survey captures their experiences, awareness, and perceptions regarding cyber offences and the effectiveness of current legal remedies.

The study also incorporates secondary data sources, such as Law Commission reports, NCRB statistics, UN and ESCAP publications, and scholarly commentaries, to assess the prevalence of cyber victimization and the adequacy of legal mechanisms. Comparative analysis of international practices, including those in the UK, EU and USA is used to identify gaps and suggest potential reforms for India.

By combining legal analysis, comparative study and empirical research, this methodology enables a comprehensive evaluation of whether India's existing legal system adequately addresses cyber offences against women and provides a basis for recommending improvements in legislation and policy.

VIII. Legal Provisions Addressing Cyber Offences

The Indian legal system addresses cyber offences against women through a patchwork of provisions:

- **Information Technology Act, 2000:**
- §66C (identity theft), §66D (cheating by personation), §66E (violation of privacy), §67 and §67A (obscenity and sexually explicit material).
- **Indian Penal Code, 1860 / Bharatiya Nyaya Sanhita, 2023:**
- Provisions relating to stalking (§354D IPC/§79 BNS), voyeurism (§354C IPC/§77 BNS), outraging modesty (§354 IPC/§73 BNS), and criminal intimidation (§506 IPC/§351 BNS).
- **Case law:**
- In *State of West Bengal v. AnimeshBoxi* (2018), the court convicted the accused for circulating private videos of a woman without consent, applying both IT Act and IPC provisions.
- In *ShreyaSinghal v. Union of India* (2015), the Supreme Court struck down §66A IT Act, which was misused to curb free speech, but indirectly made takedown procedures more formal and complex for women seeking immediate relief.

These provisions demonstrate that while statutory tools exist, they were largely drafted for general offences and adapted to cover gendered harms, often leaving interpretative gaps.

Challenges in Enforcement

Despite the presence of statutory mechanisms, women victims face multiple barriers in accessing justice:

- a) Reporting Difficulties:** Many women are hesitant to report due to fear of social stigma, lack of trust in law enforcement, and concerns over confidentiality. NCRB data shows under-reporting remains a pervasive issue.
- b) Delay in Takedowns:** Although the IT Rules 2021 (amended 2022–2023) impose obligations on intermediaries for grievance redressal, women frequently experience delays in removal of offensive content, particularly on encrypted or foreign platforms.
- c) Gender-Insensitive Policing:** Studies and anecdotal evidence point to dismissive attitudes of some police officials towards women complainants, further discouraging reporting.
- d) Digital Literacy Gaps:** Lack of awareness about privacy settings, reporting tools, and available legal remedies limits the capacity of women, including students, to protect themselves online.

Comparative Insights

International practices show stronger, survivor-oriented approaches:

- **United Kingdom:** The Criminal Justice and Courts Act, 2015 criminalizes “revenge pornography” explicitly, with streamlined reporting processes.
- **United States:** Several states criminalize non-consensual pornography, supported by the Violence against Women Act (VAWA) provisions on cyberstalking.
- **European Union:** The Directive on Combating Violence Against Women (2022 proposal) includes specific provisions on online harassment, deepfakes, and cyber exploitation.
- **Compared to these,** India's reliance on general provisions under the IT Act and IPC/BNS appears fragmented, necessitating more tailored statutes.

VIII. Finding and Analysis

This chapter delineates the analysis of data and the research findings derived therefrom. In alignment with the stated objectives of the study, both primary and secondary data were collected and systematically examined. The research, entitled “A Critical Study of Cyber Offences against Women and the Role of Law: With Special Reference to Presidency University, Bengaluru”, involved the administration of 1000 questionnaires, which were disseminated online among the students of Presidency University. All distributed questionnaires were duly completed and returned by the respondents. The collected data have been subjected to a comprehensive analysis, wherein descriptive statistical techniques, including ratios and percentages, have been applied to interpret the responses and derive meaningful insights.

Rising Incidence of Cyber Offences Against Women

The research highlights a consistent increase in cyber offences targeting women in India. According to the NCRB Crime in India 2022 Report, cybercrime cases rose by 24.4% compared to 2021, with sexual exploitation (5.2%) and cyberstalking/bullying of women forming a significant share of total cases. Within cybercrimes specifically against women, offences such as cyber pornography, morphing of images, creation of fake profiles, and online harassment have

shown an alarming upward trend. This pattern mirrors findings of the UN ESCAP 2021 study, which documented disproportionate victimization of women in digital spaces across Asia due to structural inequalities and gendered risks. At the micro level, informal observations and discussions within Presidency University, Bengaluru, suggest that young women—particularly students—are increasingly exposed to online harassment through platforms such as Instagram, WhatsApp, and Telegram. Incidents often involve the creation of fake accounts using morphed photographs, unsolicited explicit messages, and persistent stalking. This aligns with the national data, underscoring how universities reflect broader patterns of digital victimization.

Sample Profile

The sample is dominated by younger respondents, consistent with a university-based survey. Age profiles are concentrated in the “Below 20” and “20–30” brackets. This aligns with expectations for undergraduate and early postgraduate cohorts. Gender breakdowns contextualise subsequent analysis on cyber offences targeting women.

Awareness of Cyber Offences and Reporting Pathways

A majority of respondents reported being aware of different types of cyber offences against women, while a smaller segment reported partial or no awareness. Knowledge of where to report was similarly high, though a notable minority remained unaware. Awareness must therefore be paired with clear procedural guidance for reporting.

Prevalence and Modalities of Offences

The frequency plots suggest harassment, obscene content, and impersonation as prominent categories. Platforms such as Instagram, WhatsApp, and Twitter feature prominently. Image-based platforms concentrate risks of morphing and non-consensual dissemination, while messaging platforms see higher levels of unsolicited content.

Reporting Behaviour and Barriers

Although most respondents knew where to report, not all victims of offences acted upon this knowledge. Barriers include stigma, fear of escalation, and lack of trust in authorities. This underscores the gap between awareness and actual reporting behaviour.

Demographic Correlates

Cross-tabulations show that younger age groups more frequently report certain offences, especially image-related harms. Awareness is positively but imperfectly linked to knowledge of reporting pathways. Gender patterns reveal disproportionate vulnerability among women to harassment and stalking.

Data Quality and Limitations

As a university-based convenience sample, external validity is limited. Self-reporting introduces potential underreporting of sensitive experiences and overreporting of awareness. Cross-sectional data prevent causal inference. Despite these limitations, descriptive insights are robust.

Legal and Institutional Implications

Primary prevention measures include platform-specific training, peer support networks, and bystander interventions. Strengthening reporting and legal literacy requires a clear reporting map, documentation checklist, and simplified awareness sessions on IT and IPC provisions. Universities should integrate these into orientation and grievance redressal processes.

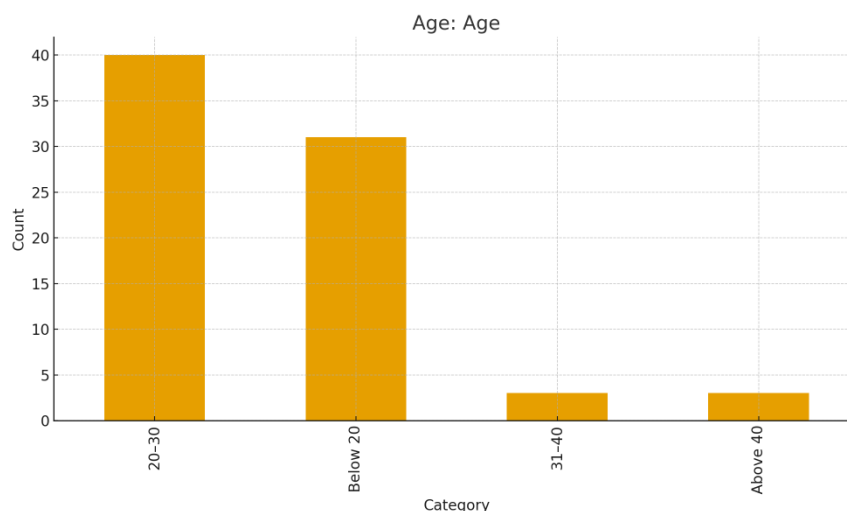


Figure 1. Age distribution of respondents

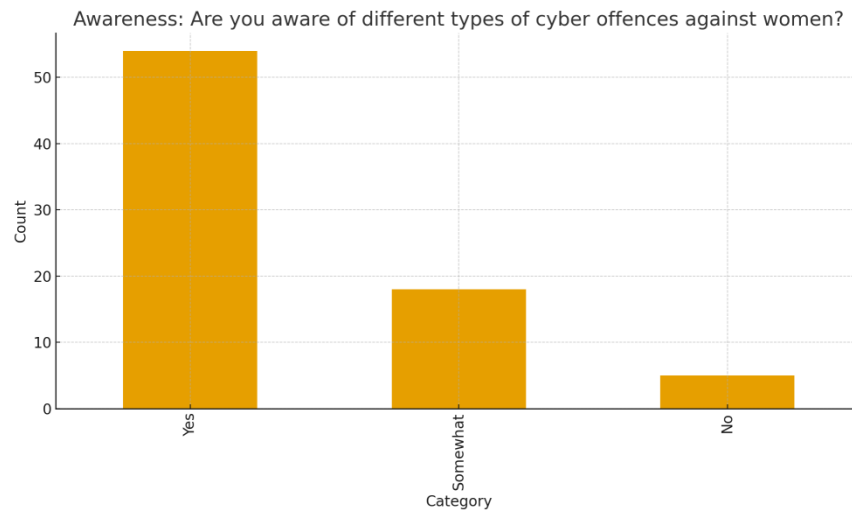


Figure 2. Awareness of cyber offences: frequency distribution

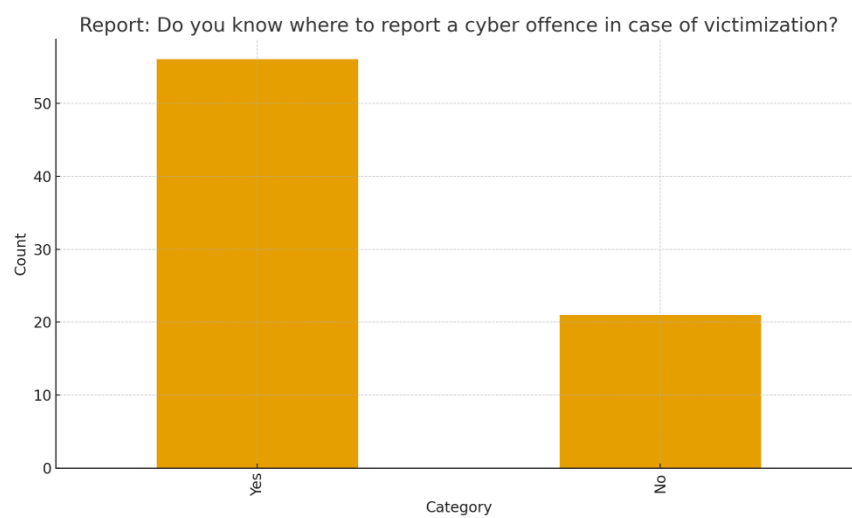


Figure 3. Knowledge of reporting pathways: frequency distribution

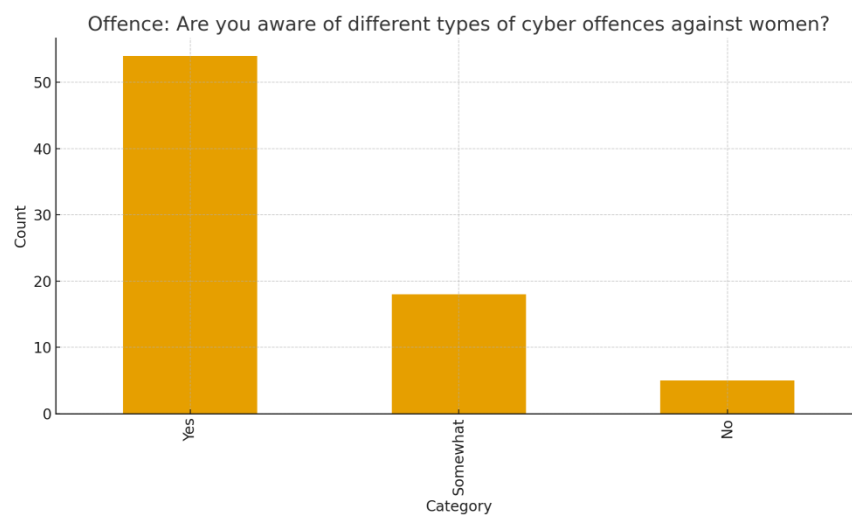


Figure 4. Offence types: frequency distribution

Critical Analysis

The study reveals high but uneven awareness, non-trivial knowledge gaps on reporting, and barriers between awareness and action. Targeted awareness, simplified reporting pathways, and integration of legal literacy into university programs can significantly improve protection against cyber offences for women.

The IT Act, though a landmark law, is outdated in dealing with sophisticated offences such as deepfakes, doxxing, and non-consensual pornography, while the BNS reorganization of offences provides clarity but not necessarily stronger protection.

The judiciary has played a proactive role in some cases, but overall enforcement suffers from systemic issues of delay, under-reporting, and lack of gender sensitivity. When compared to international frameworks, India's system lacks explicit recognition of online gender-based violence as a separate offence, which limits both data collection and targeted policy responses.

Thus, the findings suggest that while legal frameworks exist, they are fragmented, inadequately enforced, and insufficiently survivor-centric. Without comprehensive reform and increased digital literacy, women especially students and young professionals remain disproportionately vulnerable to cyber harms.

IX. CONCLUSION

The study demonstrates that cyber offences against women in India are increasing both in frequency and severity, reflecting the intersection of digital access and entrenched gender inequalities. Offences such as cyberstalking, impersonation, morphing, and circulation of intimate content not only undermine women's dignity but also create long-lasting psychological, social, and economic consequences.

India's legal response anchored in the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023), and various judicial precedents offers important safeguards. However, these laws were not originally crafted with the unique nature of online gender-based harms in mind. As a result, their application often depends on interpretive extensions rather than explicit recognition of offences. While judgments such as *Shreya Singhal v. Union of India* and *State of West Bengal v. Animesh Bhowmik* highlight judicial engagement, they also reveal structural limitations in enforcement and redressal.

At the institutional level, the experience of women at Presidency University, Bengaluru mirrors national patterns of vulnerability. Young women frequently encounter harassment through fake profiles, unsolicited explicit communication, and online stalking, yet often lack awareness of formal remedies. This underscores the broader challenge of digital illiteracy and insufficient awareness, compounded by a justice system that remains gender-insensitive and slow to respond.

Overall, while India has taken important steps through statutory amendments and intermediary regulations, its framework continues to lag behind international best practices that explicitly criminalize online gender-based violence and create survivor-centric mechanisms.

X. RECOMMENDATIONS

i. Statutory Reform

- ☐ Enact a dedicated legislation or amend the IT Act to explicitly address offences such as non-consensual pornography, deepfakes, doxxing, and cyberstalking.
- ☐ Harmonize provisions under the IT Act and BNS to reduce overlaps and ensure clarity for both victims and enforcement agencies.

ii. Strengthening Enforcement

- ☐ Establish specialized cybercrime units with gender-sensitive training in every police district.
- ☐ Mandate fast-track procedures for removal of objectionable content, with stricter timelines for social media intermediaries under the IT Rules.

iii. Awareness and Digital Literacy

- ☐ Launch nationwide campaigns focusing on safe digital practices, reporting mechanisms, and rights of women victims.
- ☐ Integrate cyber safety modules into university curricula, with Presidency University serving as a model for campus-based digital awareness.

iv. Institutional Support

- ☐ Expand victim-support mechanisms such as cyber helplines, one-stop centres, and online complaint portals that provide legal, psychological, and technical assistance.
- ☐ Encourage universities and workplaces to establish internal cyber grievance cells to support victims at the institutional level.

v. International Cooperation

- ☐ Strengthen bilateral and multilateral frameworks to address cross-border cyber offences, ensuring faster evidence-sharing and takedowns.

Ensuring women's safety in cyberspace requires more than punitive laws; it demands structural reform, proactive enforcement, survivor-friendly support systems, and cultural change. By addressing legal gaps and empowering women with digital literacy, India can transform the internet from a site of vulnerability into a space of genuine empowerment.

BIBLIOGRAPHY

1. Affairs, M. o. (n.d.). Handbook on Bhartiya Nyaya Sanhita, 2023.

2. CYRILLA. (n.d.). CYRILLA. Retrieved from <https://cyrilla.org>.
3. Dutta, L. (2023). A Study on Cybercrime Against Women: Special Reference to Dibrugarh University. *International Journal of Innovative Science and Research Technology*, 2054-2068.
4. ESCAP. (2021). The Covid-19 pandemic and violence against women in Asia and the Pacific. Policy Paper: Social Development.
5. GOI. (2025). Cyber Crimes against Women during 2017 to 2022.
6. Goyal, S. (2022, July-December). Cyber Crimes against Women and Prevention. *CHANAKYA LAW REVIEW (CLR)*, 3(2), pp. 98-108.
7. Group, W. B. (2021). Accelerating gender equality in digital development.
8. India, T. T. (2025, May). *The Times of india*.
9. India: Grievance Appellate Committees (GACs). (n.d.). Retrieved from https://digitalpolicyalert.org/change/4457-grievance-appellate-committees-gacs?utm_source=chatgpt.com.
10. JUSTICE K.S. PUTTASWAMY VS. UNION OF INDIA, (2017) 10 SCC 1 (SCC 2017).
11. Muskan. (2025). CYBERCRIME AGAINST WOMEN IN INDIA: A COMPREHENSIVE STUDY. *International Research Journal of Modernization in Engineering Technology and Science*.
12. National Crime Records Bureau, M. o. (2022). *Crime in India*. New Delhi: National Crime Records Bureau, Ministry of Home Affairs.
13. Padmavathi, L. (2015). *Lectures on Cyber Laws*. Hyderabad: Asian Law House.
14. Pathak, A., & Tripathi, P. (n.d.). *Digital Victimization of Women in cyberspace: An analysis of effectiveness of Indian Cyber Laws*. NLUJAA.
15. Shreya Singhal v. Union of India (SC MARCH 24, 2015).
16. Yadav, H. (2022). Unveiling the dark side of cyber space: A study of cybercrimes against women in India. *International Journal of Food and Nutritional Sciences*, 11(10).