CYBER CRIME AGAINST WOMEN IN INDIA

Nutan Kumari* **Sparsh Kumar***

ABSTRACT

The rapid growth of information technology and digital communication has significantly transformed the nature of crime, leading to a sharp rise in cyber offences. Among the most vulnerable sections of society affected by this transformation are women, who increasingly face harassment, exploitation, and abuse in cyberspace. Cybercrimes against women include offences such as cyber stalking, cyber pornography, image morphing, online trolling, bullying, voyeurism, and privacy infringement, which cause serious psychological, social, and reputational harm. This research paper examines the concept, forms, and current scenario of cyber crimes against women in India, supported by recent statistical data and state-wise trends. It critically analyses the existing legal framework under the Constitution of India, the Indian Penal Code, the Information Technology Act, 2000, and other relevant legislation such as the POCSO Act and the Copyright Act. The paper also highlights important judicial pronouncements, including State of Tamil Nadu v. Suhas Katti, the Puri Cyber Pornography Case, and Shreya Singhal v. Union of India, to understand the judicial approach towards cyber offences. The study identifies significant lacunae in the present legal regime, particularly the absence of specific provisions addressing emerging cyber offences such as cyber trolling and gender-based bullying. The paper concludes by suggesting legal reforms, specialised investigational cooperation to ensure effective protection of women in cyberspace and to create a safer digital environment in India.

Keywords: Cyber Crime, Cyber Fraud Against Women, Cyber Harassment, Cyber Stalking, Cyber Pornography.

*BA LLB, FIFTH YEAR, JHARKHAND RAI UNIVERSITY, RANCHI.
*ADVOCATE, CIVIL COURT, RANCHI.

INTRODUCTION

With the rapid change in information technology and the widespread use of computers, smartphones, and the internet, cybercrime has emerged as a serious threat in modern society. The increasing dependence on digital platforms for communication, banking, social interaction, and education has significantly expanded the scope of criminal activities in cyberspace.

Cybercrime can be defined as the illegal use of computers, communication devices, or internet-based networks to commit or facilitate unlawful activities. It involves offences in which computers or digital technologies are either the target or the tool used for committing the crime. Cybercrime includes a wide range of illegal activities such as identity theft, phishing scams, hacking, spreading malware, online fraud, and digital harassment. These crimes may be committed by individuals, organised groups, or even state-sponsored actors, and are often aimed at causing harm, exploiting vulnerabilities, or unlawfully accessing information. With the expansion of digital connectivity, cybercrime has become more complex and challenging to control.

CYBER CRIME AGAINST WOMEN IN THE INDIAN CONTEXT

Crimes against women have witnessed a significant increase in recent years.[1] From ancient times to the present day, women have been subjected to various forms of violence and abuse such as eve-teasing, bullying, harassment, and violation of modesty. However, in the contemporary digital era, the nature and method of committing these crimes have undergone a substantial transformation. With the advancement of technology, such offences are no longer confined to physical spaces but have increasingly shifted to the virtual world, giving rise to cybercrime against women.

TYPES OF CYBER CRIME AGAINST WOMEN IN INDIA

Cyber Stalking[2]: Cyber stalking is the practice of following someone using the internet, e-mail, or chat rooms. Cyber stalking is where the Internet or other electronic means are used to stalk or harass an individual, a group of individuals, or an organisation. It includes the making of false accusations or statements of fact, monitoring, making of threats, identity theft, damage

[1] National Crime Records Bureau, *Crime in India 2024 Report* (Ministry of Home Affairs, Government of India 2025)
[2] Debarati Halder and Jaishankar Karuppannan, *Cyber Crimes Against Women in India* (Sage Publishing 2016)

to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass. Cyber stalking does not involve any physical contact, but rather stalking through the internet.

Cyber Pornography: Female internet users are increasingly vulnerable to cyber pornography. This includes the creation, circulation, and distribution of pornographic content through online platforms, including explicit photographs and videos. The widespread availability of the internet has made it easier to commit offences related to pornography, as such content can be easily accessed, shared, and misused. In many cases, women are threatened or blackmailed through pornographic websites to obtain sexual favours or to seek revenge. One of the most common forms of such cyber offences involves the morphing of women's images into nude or sexually explicit photographs and uploading them onto pornographic platforms without consent. Due to the easy accessibility and anonymity provided by the internet, this leads to serious violations of women's privacy, dignity, and mental well-being.

Morphing[3]: Morphing is the process of an unauthorised user altering an original photograph. It is typically carried out by an unauthorised user or person using a false identity who downloads and edits the victim's original photo before uploading it. It has been proven that deceptive users are more likely to download and share edited female photographs. This crime is committed with the intent of blackmailing or defaming the victims online.

Online Trolling: Trolling is characterised as making provocative or off- topic comments to females in online communities such as newsgroups, blogs, and social media with the intention of disturbing them emotionally. It is carried out by trolls, who are professional abusers who fabricate false identification cards and utilise them for this purpose to create a cold war atmosphere.

Privacy Infringement: Privacy infringement generally means the violation of the privacy of any individual. It means taking photographs, making videos, records, private pictures, and publishing them or sending them electronically to anyone without the consent of the individual. Any violation of privacy is punishable, and legal action can be taken against it.

Voyeurism: Cybercrime voyeurism is committed when any man watches or captures the image of a woman engaged in a private act in circumstances where she has the belief of not being

[3] National Commission for Women, Cyber Crime Dat,a

observed either by the perpetrator or any other person, but those images are used to be disseminated.

Cyber Bullying: Cyber bullying means the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. The main aim and objective behind such crime may be to defame the target out of anger, hatred or frustration, or secondly, when the perpetrator wants to make fun of his friends, classmates, juniors, or unknown net friends.

STATISTICAL DATA AND CURRENT SCENARIO OF CYBER CRIME AGAINST WOMEN IN INDIA

Recent official statistics reveal that crimes against women in India remain alarmingly high, with a steady trend of incidents recorded over the past few years. According to the latest Crime in India report released by the National Crime Records Bureau, India registered approximately 4,48,211 cases of crimes against women in 2023, showing a marginal increase compared to 2022 and 2021 figures. The national crime rate for offences against women stood at 66.2 incidents per lakh female population in 2023.[4]

Among the reported crimes, cyber offences have shown a significant surge. In 2023, a total of 86,420 cases of cybercrime were registered across the country, making a 31.2% increase from the 65,893 cases reported in 2022. This rapid rise highlights how digital platforms are increasingly used to commit unlawful activities, including offences that specifically impact women, such as online harassment, image morphing, cyber pornography, and threats.[5] While fraud- related cybercrime makes up the largest share of these cases, a substantial number also involve sexual exploitation, extortion, and online harassment, which disproportionately affect female users.

The statistical data thus underscores an urgent need for stronger enforcement mechanisms, enhanced digital literacy, and robust support systems for women to report and seek redressal for cybercrimes. Despite increasing awareness and reporting mechanisms, enhanced digital literacy, and robust support systems for women to report and seek redressal for cybercrimes. Despite increasing awareness and reporting mechanisms, many incidents likely remain under-

[4] National Crime Records Bureau, Crime in India 2022-2023
[5] Ministry of Home Affairs, Government of India

reported due to stigma, fear of victim- blaming, and lack of access to cybercrime reporting portals.

STATE-WISE ANALYSIS OF CYBER CRIME AGAINST WOMEN IN INDIA

State	Nature of crime	Trend
Uttar Pradesh	Online harassment, cyber stalking, fake profiles, image morphing	High
Maharashtra	Cyber pornography, revenge porn, online blackmail	Very High
Karnataka	Social media abuse, cyber stalking, identity theft	High
Telangana	Online sexual harassment, morphing of images	High
Delhi	Cyber harassment, threats, circulation of obscene content	Very High
Rajasthan	Online abuse, cyber blackmail	Moderate
Tamil Nadu	Cyber bullying, impersonation	Moderate
West Bengal	Online harassment, fake social media accounts	moderate

The state-wise data indicates that urban and technologically advanced states report a higher number of cybercrimes against women, largely due to greater internet penetration and improved reporting mechanisms. However, lower figures in certain states do not necessarily indicate fewer crimes; instead, they reflect under-reporting, lack of awareness, and social stigma associated with reporting cyber offences.

Metropolitan regions such as Delhi, Maharashtra, and Karnataka consistently report higher incidents of cyber harassment, image morphing, and online sexual exploitation of women. The increasing accessibility of smartphones and social media platforms has further contributed to the rise of such offences across states.

LEGAL FRAMEWORK GOVERNING CYBER CRIME AGAINST WOMEN IN INDIA

The Constitution of India, 1950:[6] Article 19 and 21 of the Constitution of India provide constitutional protection to women against cybercrime. Article 19(1)(a) guarantees the fundamental right to freedom of speech and expression. However, this right is not absolute and is subject to reasonable restrictions prescribed under Article19(2) of the Constitution. Article 21 ensures the right to life and personal liberty, which includes the right of women to live with human dignity in both physical and digital spaces.

Indian Penal Code, 1860:[7] The Indian Penal Code contains several provisions that address cybercrimes against women. Sections 292 to 294 deal with offences relating to insulting the modesty of a woman. Section 354 and its sub-section (section 354Ato 354D) deal with offences relating to outraging the modesty of a woman, including sexual harassment, stalking, and voyeurism. Sections 292, 293,294, 504 and 509 also address issues related to pornography and abusive conduct. Additionally, Section 379, 405, and 420 are invoked in cases of data theft, criminal breach of trust, and cheating involving digital platforms.

Information Technology Act, 2000:[8] The Information Technology Act, 2000 provides statutory provisions to address cyber offences. Section 66A earlier dealt with sending offensive messages through communication services. Section 65 relates to tampering with computer source documents, while Section 70 addresses unauthorised access to protected systems and confidentiality and privacy, including online stalking. Sections 43A and 66 of the IT Act, read with Sections 379 and 406 of the IPC, deal with data hacking and unauthorised access. Sections 43B, 66E and 67C address data theft, violation of privacy, and the obligation of intermediaries to preserve the publication or transmission of sexually explicit content in electronic form.

[6] Constitution of India 1950
[7] Indian Penal Code 1860
[8] POCSO Act 2012

The Copyright Act, 1957: Section 63B of the Copyright Act, 1957 protects against data theft and misuse of computer programs. It penalises any person who knowingly makes use of an infringing copy of a computer program, thereby safeguarding digital intellectual property, including that belonging to women.

Protection of Children from Sexual Offences (POCSO) Act 2012: The POCSO Act, 2012 offers protection to girl children from sexual offences, including those committed through digital means. Section 3 deals with penetrative sexual assault, while Section 3 deals with penetrative sexual assault, while Section 5 addresses aggravated sexual assault. Section 7 defines sexual assault, and Section 9 covers aggravated sexual assault. Section 11 criminalises sexual harassment of a child for pornographic purposes.

LEGAL REMEDIES AVAILABLE TO VICTIM OF CYBER CRIME AGAINST WOMEN IN INDIA

Sexual Harassment – Section 354A, Indian Penal Code, 1860:[9] Under Section 354A of the Indian Penal Code, 1860, a man shall be held guilty of the offence of sexual harassment if he commits any of the following acts:

1. Makes physical contact and advances involving unwelcome and explicit sexual overtures; or
2. Demands or requests sexual favours; or
3. Shows pornography to a woman against her will; or
4. Makes sexually coloured remarks.

The first three acts of sexual harassment are punishable with rigorous imprisonment for a term which may extend up to three years, or with fine, or with both. The fourth act, namely making sexually coloured remarks, is punishable with imprisonment for a term which may extend to one year, or with fine, or with both.

Stalking - Section 354D, Indian Penal Code, 1860: Section 345D of the IPC defines stalking as an act committed by a man who:

1. Follows a woman and contacts, or attempts to contact her, to obtain personal information despite her clear indication of disinterest; or

[9] Indian Penal Code,1860

2. Monitors the use of the internet, email, or any other form of electronic communication by a woman.

Any person found guilty of stalking shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine upon first conviction.

Violation of Privacy - Section 66E, Information Technology Act, 2000:[10] Section 66E of the Information Technology Act, 2000 penalises the intentional capturing, publishing, or transmission of images of a person's private body parts without consent. The offence is punishable with imprisonment which may extend up to three years, or with a fine not exceeding two lakh rupees, or with both.

Cheating by Personation - Section 66D, Information Technology Act, 2000: Section 66D of the IT Act deals with cheating by personation through the use of any communication device or computer resource. Any person committing such an offence shall be punishable with imprisonment which may extend to three years and with a fine which may extend to one lakh rupees, or with both.

Identity Theft - Section 66C, Information Technology Act, 2000: Under Section 66C of the IT Act, any individual who fraudulently or dishonestly makes use of another person's electronic features shall be punished with imprisonment which may extend to three years and with a fine which may extend to one lakh rupees, or with both.

Voyeurism - Section 354C, Indian Penal Code, 1860: Voyeurism under Section 354C IPC involves watching, capturing, or disseminating the image of a woman engaged in a private act in circumstances where she reasonably expects privacy. A person committing this offence shall be punished on first conviction with imprisonment of either description for a term not less than one year, which may extend to three years, along with a fine. For a second or subsequent conviction, the punishment shall be imprisonment for a term not less than three years, which may extend to seven years, along with a fine. Further, where a woman consents to the capturing of images or performance of an act but does not consent to the dissemination of such material, any unauthorised dissemination shall constitute an offence under this section.

[10] Information Technology Act,2000

Publishing or Transmitting Obscene Material in Electronic Form- Section 67, Information Technology Act,2000

Section 67 of the IT Act penalises the publication or transmission of obscene material in electronic form. Any person who publishes or transmits lascivious material, appeals to prurient interests, or tends to deprave and corrupt individuals likely to access it shall be punished on first conviction with imprisonment which may extend to three years and with a fine which may extend to five lakh rupees.

Publishing or Transmitting Sexually Explicit Content - Section 67A, Information Technology Act, 2000: Section 67A addresses the publication or transmission of content containing sexually explicit acts or conduct in electronic form. The offence is punishable on first conviction with imprisonment which may extend to five years and with a fine which may extend to ten lakh rupees.

Breach of Confidentiality and Privacy - Section 72, Information Technology Act, 2000:[11] Section 72 of the IT Act provides punishment for the unlawful disclosure of electronic records or personal information. Any person who discloses such information without the consent of the concerned individual shall be punishable. Any person who discloses such information without the consent of the concerned individual shall be punishable with imprisonment which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

JUDICIAL APPROACH AND LANDMARK CASE LAWS

State of Tamil Nadu v Suhas Katti:[12] The case of State of Tamil Nadu v. Suhas Katti is a landmark judgment dealing with online harassment and the circulation of obscene and defamatory content against a woman. In this case, the accused posted obscene, defamatory, and offensive messages about a divorced woman in a Yahoo chat group. He also created a fake email account in the victim's name and used it to send messages to various individuals, thereby damaging her reputation.

As a result of these online postings, the victim was subjected to continuous harassment and received several unwanted and offensive phone calls from strangers who believed that she was soliciting. Distressed by the situation, the victim filed a complaint before the Egmore Court in

[11] Cyber Crime Reporting Portal, Ministry of Home Affairs
[12] State of Tamil Nadu v. Suhas Katti (2004)

February 2004. Following the complaint, the Chennai police Cyber Crime Cell traced and arrested the accused.

The court found the accused guilty and convicted him under Section 469 and 509 of the Indian Penal Code, 1860, for defamation and outraging the modesty of a woman, along with Section 67 of the Information Technology Act, 2000, for publishing obscene material in electronic form.

Puri Cyber Pornography Case:[13] The Puri Cyber Pornography case marked the first conviction for cyber pornography in the State of Odisha. In this case, the accused, Jayant Kumar Das, an RTI activist, acted out of personal vengeance against the complainant, Biswajit Patnaik, a journalist. The accused created a fake email account and a false online profile in the name of the complainant's wife and posted obscene remarks through it. He further linked this fabricated profile to an American pornographic website and publicly displayed the victim's mobile phone number on the site.

As a consequence of these actions, the victim and his family were subjected to repeated obscene messages and unsolicited phone calls, causing severe mental harassment. Disturbed by the continuous harassment, the journalist lodged a FIR at the Baselisahi Police Station in Puri in July 2012. The investigation was subsequently transferred to the Cyber Crime Cell of the Odisha Crime Branch in August 2012. Following a detailed inquiry, the accused was arrested on 18 September 2012. The Puri Sub-Divisional Judicial Magistrate Court found the accused guilty and sentenced him to 6 years of imprisonment under Section 66C, 67 and 67A of the Information Technology Act, 2000, for identity theft and publishing obscene and sexually explicit material in electronic form.

Shreya Singhal v Union of India:[14] Shreya Singhal v Union of India is a landmark judgment of the Supreme Court of India dealing with freedom of speech and expression in cyberspace. The case holds significant importance in the context of cybercrime against women, particularly on social media platforms, where online abuse and harassment pose serious threats to women's safety and dignity.

In this case, the Constitutional validity of Section 66A of the Information Technology Act, 2000 was challenged. The petitioners contended that Section 66A was vague, arbitrary, and

[13] Puri Cyber Pornography Case (2012)
[14] Shreya Singal v. Union of India (2015) 5 SCC 1

excessively broad, and that it was being grossly misused by authorities to curb legitimate freedom of speech and expression on the internet. Accepting these arguments, the Supreme Court struck down Section 66A as unconstitutional on the ground that it violated Article 19(1)(a) of the Constitution of India and was not saved by the reasonable restrictions under Article19(2).

While the court acknowledged the draconian nature of the provision, the judgment also raised an important debate. The question remains whether the Supreme Court could have utilised this opportunity to reframe or recommend a more precise legal provision to regulate certain harmful forms of online speech. In India, cyberbullying, trolling, online gender-based harassment, phishing, and vishing have become increasingly rampant, particularly affecting women in cyberspace.

From a broader perspective, the court could have considered the therapeutic jurisprudential value of Section 66A by guiding the legislature towards formulating a balanced law that protects freedom of expression while simultaneously addressing harmful online behaviour. Such a legal framework could have strengthened the protection of women against cyber abuse without compromising constitutional rights.

CONCLUSION AND SUGGESTIONS

In the Indian context, incidents of cybercrime against women are increasing at an alarming rate. With the rapid growth of digital platforms, new forms of offences such as cyber trolling, cyber bullying, and online gender-based harassment have emerged as serious threats to women in cyberspace. However, the existing legal framework, particularly the Information Technology Act,2000, does not comprehensively address many of these offences, and the investigation mechanisms remain inadequate. The absence of specific provisions dealing with cyber trolling and gender-based bullying highlights significant lacunae in the present law.

Cyber stalking has also become a grave concern, requiring stricter legal regulation. There is an urgent need to amend the Information Technology Act,2000, to expressly recognise and penalise such emerging cyber offences[15]. Further, considering the seriousness and far-reaching impact of cybercrimes against women, a majority of these offences should be made non-

[15] United Nations Women, Online Violence Against Women Reports

bailable to act as a deterrent.[16] The establishment of specialised cybercrime investigation cells with trained personnel is essential for effective enforcement of the law.

Additionally, there is a pressing need for separate and comprehensive legislation dedicated to cybercrimes, particularly those affecting women. Incorporating a robust data protection regime within the legal framework would further strengthen the protection of women's privacy and personal information in the digital space. Specialised training programmes must be provided to police officers and investigating agencies to enable them to handle cybercrime cases in a gender-sensitive and technologically informed manner.

The judiciary[17] also has a crucial role to play by adopting a progressive and victim-centric approach while interpreting cyber laws to ensure effective justice. Moreover, the Indian government should actively pursue bilateral and multilateral cooperation with other countries to facilitate information sharing and coordination in the investigation of cross-border cybercrimes. Such combined efforts are necessary to create a safer and more secure cyberspace for women in India.

[16] NITI Aayog, Digital Governance Studies
[17] Law Commission of India Reports