



CYBER CRIME AGAINST WOMEN

LEGAL CHALLENGES AND EFFECTIVE RESPONSES IN INDIA

Kanika Rathore

LL.M (law) Government law college ajmer

Dr. Bhimrav ambedkar University

ABSTRACT : The rapid expansion of digital technology has transformed social interactions but has simultaneously intensified cyber crime , particularly against women. Cyber crime such as cyber stalking, online harassment, morphing, revenge pornography, identity theft, and cyber defamation disproportionately affect women, leading to psychological trauma and violation of fundamental rights. Despite the existence of legal framework under the Information Technology Act,2000 and the Bharatiya Nyaya Sanhita, effective implementation remains a challenge. This article critically examines the nature of cyber crime against women in India, evaluates existing legal provisions, identifies enforcement gaps, and suggests legal and policy reforms to ensure effective protection and justice.

KEYWORDS: Cyber Crime, Women, Digital Violence, Information Technology Act, Cyber Law India.

WHAT IS CYBER CRIME ?

The digital revolution has reshaped communication and Education they are connected . However this also has to do with things like education and commerce. Created new avenues for criminal activities. Women, due to social vulnerability and gender-based discrimination is a problem. People who face discrimination is very serious offence. Cyber crime against women are not merely technology offences but represent a serious form of gender based violence violating, dignity, privacy and personal liberty. The increasing penetration of smartphone and social media platforms has intensified such crime, making legal intervention indispensable.

CONCEPT AND NATURE OF CYBER CRIME AGAINST WOMEN :

Cyber crime against women is when someone does something to a woman using computer or phones. This can hurt a woman's feeling and reputation. It is also a violation of her privacy. The criminal mind people who do these things can hide who they are which makes it hard to catch them. They can also send things about a woman to a lot of people very quickly due to the internet network service. It is hard to say which country's laws should be used to stop them. They do even worse for the women who are affected by cyber crime against women. It is a big problem of crime cause severe psychological and emotional harm, often resulting in fear, trauma and social isolation of victims. Due to under reporting social stigma, and technological, cyber crime against women remain inadequately addressed, posing a serious threat to women's fundamental rights and digital safety.

MAJOR FORMS OF CYBER CRIME AGAINST WOMEN:

- [1] CYBER STALKING = Cyber stalking involves repeated and persistent monitoring, following or contacting a woman through electronic communication with the intention to harass, intimidate, or instill fear.
- [2] ONLINE SEXUAL HARASSMENT = Online sexual harassment refers to unwanted sexually explicit messages, images, video or remarks communicated through digital platforms.
- [3] REVENGE PORN (NON-CONSENSUAL SHARING OF INTIMATE IMAGES) = Revenge porn involves the publication or transmission of images or video of a woman without her consent, often with the intent to harm her reputation or dignity.
- [4] MORPHING AND MANIPULATION OF IMAGES = This offence involves digitally altering or manipulating a woman's photography to create obscene or sexually explicit content and circulating it online.
- [5] IDENTITY THEFT AND IMPERSONATION = Identity theft occurs when a woman's personal information, photographs, or online identity is misused to create fake profiles or commit fraud.
- [6] ONLINE DEFAMATION = Online defamation includes publishing false statements, allegations or rumours about a woman through digital platforms, damaging her reputation.
- [7] ONLINE THREAT AND CYBER BLACKMAIL = This form involves threatening a woman with harm, exposure of private content, or defamation to extort money, favours or silence her.
- [8] DOXXING = Doxxing refers to the public disclosure of a woman's private or personal information such as address, phone number or working place without consent, exposing her to danger.

LEGAL FRAMEWORK IN INDIA :

The legal framework in India to combat cyber crime against women is based on a combination of the Information Technology Act 2000, the newly enacted Bharatiya Nyaya Sanhita, 2023 and constitutional safeguards. The IT Act 2000 serves as the primary cyber law, addressing offences such as identity theft (section 66C), online impersonation and fraud (section 66D), violation of privacy (section 67 and 67A), which are commonly involved in cyber crime against women.

The Bharatiya Nyaya Sanhita, 2023, which has replaced the Indian Penal Code, retains key gender-protective provisions relating to sexual harassment, voyeurism, cyber stalking, insult to the dignity of women, and criminal intimidation committed through electronic means. Procedural support is provided by the Bharatiya Nagarik Suraksha Sanhita 2023, which strengthens investigation and reporting mechanisms for cyber offences. Additionally, constitutional guarantees under Article 14, 15 and 21 ensure equality, non-discrimination, dignity and the right to privacy of women in the digital space. Despite this framework, effective enforcement remains a challenge, highlighting the need for stronger implementation and gender-sensitive cyber justice mechanisms.

CHALLENGES IN ADDRESSING CYBER CRIME AGAINST WOMEN:

Cyber crime against women is difficult to address due to under-reporting caused by social stigma and fear of victim-blaming, anonymity of offender, and the borderless nature of cyberspace which complicates investigation and jurisdiction. Rapid technological advancement outpacing existing laws, coupled with limited cyber forensic capacity, lack of gender-sensitive enforcement and delays in content removal result in low conviction rates and continued victimization of women.

UNDER-REPORTING = Under-reporting is a major challenge in addressing cyber crime against women, primarily due to social stigma, fear of victim-blaming, damage to reputation and lack of awareness about legal remedies. Many women hesitate to report cyber offences because of societal pressure, lack of family support and fear of insensitive handling by law-enforcement agencies. Additionally, limited digital literacy and

uncertainty about evidence preservation further discourage reporting, resulting in low registration of case and weakening the effectiveness of the cyber justice system.

LACK OF CYBER AWARENESS: Lack of cyber awareness is a significant challenge in addressing cyber crime against women, as many women are unaware of safe online practices, legal remedies and reporting mechanisms. Limited digital literacy, especially regarding privacy setting, data protection and evidence preservation, makes women more vulnerable to online abuse and exploitation. This lack of awareness often result in delayed reporting or non-reporting of cyber offence, allowing perpetration to continue their activities with impunity.

WEAK ENFORCEMENT : Weak enforcement remains a major challenges in addressing cyber crime against women due to inadequate implementation of cyber laws, lack of coordination among enforcement agencies and sufficient technical training of law-enforcement personnel. Delays in investigation, low conviction rates, and ineffective monitoring of online platforms further reduce deterrence. As a result, despite the existence accountability, undermining women's confidence in the cyber justice system.

INVESTIGATION DIFFICULTIES : Investigation of cyber crime against women faces serious difficulties due to the anonymity of offender use of fake identities encrypted platforms and cross-border nature of cyber offences. Challenges in digital evidence collection, preservation and authentication further weaken investigations. Limited cyber forensic infrastructure, shortage of trained personal and delays in tracing online activities often result in prolonged investigation and low conviction rates, reducing the effectiveness of legal response to cyber crimes against women.

ROLE OF JUDICIARY IN CYBER CRIME AGAINTS WOMEN :

The judiciary play an important role in dealing with cyber issues. Cyber problems are a deal and the judiciary is there to help figure out what to do. Cyber is a word that mean computer and internet and when we talk about cyber we are talking about the judiciary and cyber issues. The judiciary make decisions, about cyber problems. That is a big responsibility. Cyber issues are not going away.

Crime against women by interpretation cyber laws in a gender-sensitive manner and extending constitutional protection to the digital sphere. Court have started to see that cyber crime against women is a problem to involve women rights to be treated with respected to have privacy and to be free. The court have helped women who're victim by making sure the police investigate quickly by removing bad content from the internet and by keeping women identities safe. The court also found the way to make the laws work better for women by interpreting them in a way that help women even when the lawsre not perfect. cyber crime against women is an issue and the courts are doing something about it. The court are working to protect women from cyber crime and makes sure they have the rights they deserve, like dignity, privacy and personal liberty. due to there differ situations there are some mains points to knowing the major factors of judiciary in cyber crime in against women.

- Interprets cyber laws in gender-sensitive and purposive manner to protect women in dignity spaces.
- Extends constitutional rights such as dignity, privacy and personal liberty to cyberspace under Article 21.
- Fill legislative gaps gap by applying existing provisions of the IT Act and criminal law to emerging cyber offences.
- Recognize cyber crime against women as a form of gender based violence, not merely a technical offence.
- Strengthens victim protection by issuing direction for speedy investigation, content takedown and confidentiality of victims.
- Ensures accountability of law enforcement agencies and digital platform in handling cyber offences against women.
- Promotes judicial activism to address under-reporting weak enforcement, and insensitive, handling of complains.
- Enhances access to justice by adopting a victim-centric and rights-based approach.

SUGGESTION AND RECOMMENDATION :

Cyber crime against women require a comprehensive and multi-layered responded integrates legal, technological, institutional and social measure. the following recommendation are proposed to effective compact this growing threat :

[1] Strengthening Cyber Awareness and digital Literacy = There is an urgent need to enhance cyber awareness. Women can benefit from literacy program that are well organized program to teach women about things. Like keeping their information online. They learn how to use internet in a way. They also learn how to spot profiles and avoid people who are trying to trick them which is called phishing. Additionally they learn about harassment and how to deal with it.

[2] Simplification of Reporting and Complaint Mechanisms :

centric. Online complaint portals, helpline and mobile application should be widely publicized to address the issue of under-reporting of cyber crime against women.

[3] Effective Implementation of Cyber Laws :

Existing cyber laws must be enforced strictly and uniformly. Provision under the Information Technology Act and Bharatiya Nyaya Sanhita should be applied rigorously to ensure deterrence and accountability of offenders.

[4] Capacity Building of Law Enforcement Agencies :

Law enforcement authorities and cyber crime investigation unites require continuous technical training and gender-sensitization. Enhanced expertise in digital forensics and evidence collection is essential for successful prosecution.

[5] Accountability of social media and digital platforms :

Social media intermediaries should be legally mandated to adopt proactive monitoring, prompt content removal and transparent grievance redressal mechanism to curb online abuse and harassment targeting women.

[6] Speedy Trial and Judicial Sensitization :

The establishment of fast-track court for cyber crimes against women is recommended to ensure timely justice. Judicial training program should focus on the evolving nature of cyber offence and their gender-specific impact.

[7] Societal Reform and Promotion of Ethical Online Behavior :

Addressing cyber crime against women also requires societal transformation. Victim-blaming attitude must be discouraged and ethical responsible online conduct should be promoted through education and public discourse.

CONCLUSION :

Cyber crime has emerged as a serious and multifaceted challenges in digital Era, posing significant threat to women's dignity, privacy, safety and mental well being. This study highlights that offence such as online harassment, cyberstalking and digital exploitation are not merely technological issues rooted in gender based violation in society. The presence of legal provisions under the Information Technology Act 2000, and Bharatiya Nyaya Sanhita 2023 effective implementation remains limited due to under-reporting lack of cyber awareness and investigation difficulties.

The research underscores that legal mechanisms alone are insufficient to address this problem. A coordinated approach are insufficient to address this problem. A coordinated approach involving gender-sensitive law enforcement, responsive judicial gender-sensitive law enforcement, responsive judicial interpretation, technology safeguard and public awareness is essential. Ensuring a safe digital environment is crucial for women's participation and empowerment in cyberspace. Therefore, combination cyber crime against women must be threatened as a collective legal The research underscores that legal mechanisms alone are insufficient to address this problem. A coordinated approach involving gender-sensitive law enforcement, responsive judicial interpretation, technological safeguards, and public awareness is essential. Ensuring a safe digital environment is crucial for women's participation and empowerment in cyberspace. Therefore, combating cyber crime against women must be treated as a collective legal and social responsibility to achieve a secure, inclusive, and just digital future and social responsibility to achieve a secure, inclusive and digital future.

“The study cover statutory law, judicial interpretation, government data and international human right perspective.”

REFERENCE :

- [1] The Information Technology Act 2000
- [2] The Bharatiya Nyaya Sanhita 2023, (BNS)
(Enforcement w.e.f. 1 July 2024 – replacing the Indian penal code, 1860)
- [3] The Protection of women from sexual Harassment at workplace Act 2013
- [4] State of Tamil Nadu v. Suhas Katti (2004)
- [5] Justice K.S. Puttaswamy v. Union of India (2017)
- [6] national crime record bureau (NCRB)
- [7] National commission for women (NCW)
- [8] Debarati Halder – Cyber Crime against women in India
- [9] R.K. Chaubey, An introduction to cyber crime and cyber law
- [10] K.S Verma, Cyber Crime and Law
- [11] Jonathan Rosenoer, Cyber Law: The Law of the Internet
- [12] Reading Research of Article on gender based cyber violence
- [13] UN Women report on online violence against women
- [14] Intermediary Guidelines & Digital Media Ethics Code 2021
- [15] Clive Gringras – The Laws of the internet