Central University of Kashmir Law Review
Vol. 4 (2024)
eISSN: 2583-6935
pp. 133-147

Cyber Crimes against Women in India: An Analysis

Mohammadi Tarannum[*]

Abstract

Cybercrime against women is a growing threat in India, exacerbated by the rapid expansion of the digital landscape. Women are subjected to various forms of online harassment, cyberstalking, identity theft and non-consensual distribution of explicit content, which have serious psychological, emotional and social consequences. Despite existing legal frameworks such as the Information Technology Act 2000, women are often inadequately protected due to enforcement problems and gaps in legislation. Addressing this issue requires a multi-pronged approach that includes improving digital literacy, strengthening legal protections and promoting collaboration between government agencies, law enforcement and civil society. By addressing the root causes and implementing comprehensive solutions, we can create a safer and more inclusive digital environment for women in India.

Keywords: Cybercrime, Women's Safety, Cyberstalking, Revenge Pornography, Digital Literacy, Legal Protection

1. Introduction

In recent years, India has witnessed a significant rise in cybercrime, with women being disproportionately targeted. The advent of technology and the widespread use of the internet have opened up new avenues for criminals to exploit vulnerable individuals, particularly women.[1] Cybercrime against women encompasses various forms of harassment, stalking, bullying, identity theft, non-

[*] Vice Principal, Surendranath Law College, Affiliated to University of Calcutta, West Bengal, India. email: dr.mtsnlcollege@gmail.com

[1] Kumar, Sanjeev, and Anupam Manhas. "Cyber crimes in India: Trends and prevention." *Galaxy International Interdisciplinary Research Journal* 9, no. 05 (2021): 363-370.

consensual dissemination of explicit content, and online grooming.[2] As the digital landscape expands, so too does the risk of cyber threats, making it imperative to address these issues with urgency and precision.

This article sheds light on the prevailing issue of cybercrime against women in India, highlighting its causes, impact, and potential solutions. It also examines the legal framework in place to combat these crimes, the challenges faced in enforcement, and the necessary steps to ensure a safer digital environment for women.

2. Cybercrime: Definition and Scope

Cybercrime, a term with no universally accepted definition, broadly refers to criminal activities involving computers and the internet.[3] According to the Merriam-Webster Dictionary, cybercrime includes

> "criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer, especially to illegally access, transmit, or manipulate data."

Cybercrime against women in India manifests in several forms, each posing unique challenges to law enforcement and the victims involved.[4] These crimes often exploit the anonymity provided by the internet, allowing perpetrators to harass, intimidate, and manipulate women without immediate fear of retribution.[5]

[2] Halder, Debarati, and Karuppannan Jaishankar, eds. *Cyber crime and the victimization of women: Laws, rights and regulations: Laws, rights and regulations*. Igi Global, 2011.

[3] Phillips, Kirsty, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. "Conceptualizing cybercrime: Definitions, typologies and taxonomies." *Forensic sciences* 2, no. 2 (2022): 379-398.

[4] Uma, S. "Outlawing cyber crimes against women in India." *Bharati Law Review* 5, no. 4 (2017): 103-116.

[5] Chudasama, Dhaval, and Neha Dhrupalkumar Gajjar. "Cyber Crime Against Women." *National Journal of Cyber Security Law* 6, no. 2 (2023): 50-59p.

3. Types of Cybercrime against Women

(a) Online Harassment and Cyberbullying

- **Sharing Explicit Content Without Consent**: One of the most common forms of online harassment is the non-consensual sharing of explicit images or videos.[6] This form of exploitation not only violates privacy but also leads to severe emotional and psychological trauma.
- **Online Stalking and Persistent Harassment**: Cyberstalkers frequently use social media platforms to track, harass, and intimidate their victims.[7] This can include sending unwanted messages, making threatening comments, or continuously monitoring the victim's online activities.
- **Threats, Abusive Messages, and Hate Speech**: Women often face threats of physical harm, abusive language, and hate speech online, which can escalate to real-world violence.[8]

(b) Revenge Pornography

- **Non-Consensual Sharing of Intimate Images/Videos**: Revenge pornography involves the distribution of sexually explicit images or videos of individuals without their consent.[9] Often, these images are shared by ex-partners as a form of retribution.
- **Blackmailing and Extortion Using Explicit Content**: Perpetrators may use explicit content to blackmail women,

[6] Walker, Kate, and Emma Sleath. "A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media." *Aggression and violent behavior* 36 (2017): 9-24.

[7] Pietkiewicz, Michał, and Malwina Treder. "Cyberstalking in social media–Polish view." *Journal of Modern Science* 3 (38) (2018): 29-40.

[8] Sobieraj, Sarah. *Credible threat: Attacks against women online and the future of democracy*. Oxford University Press, 2020.

[9] Powell, Anastasia, Nicola Henry, Anastasia Powell, and Nicola Henry. "Beyond 'revenge pornography'." *Sexual violence in a digital age* (2017): 117-152.

demanding money or further explicit material under the threat of public exposure.[10]

(c) Online Financial Fraud

- **Phishing Scams Targeting Women's Financial Information**: Women are often targeted in phishing scams where criminals attempt to steal sensitive information, such as banking details, through deceptive emails or messages.[11]
- **Identity Theft and Credit Card Fraud**: Cybercriminals may also steal a woman's identity to commit financial fraud, including unauthorized credit card transactions or applying for loans in her name.[12]

(d) Cyberstalking

- **Persistent Online Surveillance, Tracking, and Intimidation**: Cyberstalkers engage in continuous monitoring of a woman's online presence, often leading to fear and anxiety.[13] This can involve tracking social media activity, hacking into accounts, or sending relentless messages.
- **Manipulative Behavior and Psychological Distress**: Cyberstalkers often use manipulation to exert control over their victims, causing significant psychological harm.[14]

[10] Hussein, Omar Abdulsalam. "Cyber Blackmail Crime against Women-A Case Study." *Journal of Positive School Psychology* 6, no. 3 (2022): 6882-6893.

[11] Button, Mark, and Cassandra Cross. *Cyber frauds, scams and their victims*. Routledge, 2017.

[12] Smith, Russell G. "Identity theft and fraud." In *Handbook of internet crime*, pp. 273-301. Willan, 2013.

[13] Rapisarda, Sabrina S., and Kimberly R. Kras. "Cyberstalking." *Handbook on Crime and Technology* (2023): 303-333.

[14] Attrill-Smith, Alison, and Caroline Wesson. "The psychology of cybercrime." *The Palgrave handbook of international cybercrime and cyberdeviance* (2020): 653-678.

(e) Online Trafficking and Exploitation

- **Recruitment of Victims Through Social Media Platforms**: Traffickers use social media to recruit women and girls for exploitation, often luring them with false promises of employment or relationships.[15]
- **Online Grooming for Sexual Exploitation**: Predators groom women and young girls online, gaining their trust before coercing them into sexual exploitation.[16]

4. Statutory Laws Regulating Cybercrimes against Women in India

India has implemented several laws to address cybercrime, with specific provisions designed to protect women from online harassment, abuse, and exploitation. However, the effectiveness of these laws is often hampered by issues related to enforcement and the rapidly evolving nature of cyber threats.

(a) Information Technology Act, 2000 (IT Act)

The IT Act is India's primary legislation governing cybercrime. It includes several provisions that address offenses related to cybercrime against women:

- **Section 66E**: Punishes the non-consensual capturing, publishing, or transmitting of intimate images of a person.
- **Section 66A**: Initially dealt with sending offensive messages online, including those with sexual content, but was struck down by the Supreme Court in 2015 for being unconstitutional.
- **Sections 67, 67A, 67B**: Criminalize the publishing or transmission of sexually explicit content, including child pornography, online.
- **Section 67C**: Requires intermediaries to preserve and retain information to aid in investigations related to cybercrime, including offenses against women.

[15] Geldenhuys, Kotie. "The role of social media in facilitating human trafficking." *Servamus Community-based Safety and Security Magazine* 112, no. 7 (2019): 18-20.

[16] Ali, Sana, Hiba Abou Haykal, and Enaam Youssef Mohammed Youssef. "Child sexual abuse and the internet—a systematic review." *Human Arenas* 6, no. 2 (2023): 404-421.

(b) Protection of Women from Domestic Violence Act, 2005

While not specifically focused on cybercrime, this act acknowledges the importance of addressing technology-related abuse. It provides protection against online harassment and allows for the issuance of protection orders to prevent electronic communication that causes mental or emotional distress.

(c) Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013

This law addresses sexual harassment in the workplace, including online harassment. It mandates employers to establish mechanisms to prevent and address such cases and provides a framework for complaints and redressal.

5. Prevalent Forms of Cybercrime Against Women

(a) Online Harassment and Abuse

The internet, particularly social media platforms, has become a breeding ground for harassment and abuse. Women are frequently subjected to offensive comments, threats, hate speech, and character assassination.[17] The anonymity provided by online platforms emboldens perpetrators, making it easier for them to engage in such behavior without immediate consequences.

(b) Cyberstalking

Stalking, traditionally a physical crime, has evolved into a digital menace. Cyberstalkers use various means to track, monitor, and intimidate their victims, causing severe distress and anxiety.[18] This includes incessant messages, unsolicited emails, and tracking the victim’s online activities. The psychological impact of cyberstalking can be profound, often leading to mental health issues such as anxiety, depression, and post-traumatic stress disorder (PTSD).

[17] Jane, Emma A. “Online abuse and harassment.” *The international encyclopedia of gender, media, and communication* 116 (2020).

[18] Miftha, Ameema. “The social, legal, and technical perspectives of cyberstalking in India.” (2024).

(c) Revenge Porn

Revenge porn, or the non-consensual sharing of intimate images or videos, is a particularly distressing form of cybercrime that disproportionately affects women.[19] This violation of privacy inflicts emotional trauma and can have severe social and professional consequences. Victims often face public shaming, social ostracization, and even job loss due to the exposure of such content.

(d) Online Grooming

Online grooming involves predators exploiting the anonymity of the internet to manipulate women and young girls for sexual exploitation.[20] Predators often establish fake profiles, pretending to be someone else to gain trust, and gradually coerce victims into engaging in explicit conversations or sharing compromising material. The impact on victims is devastating, often leading to long-term psychological damage.

6. Contributing Factors to Cybercrime against Women

(a) Gender Inequality

India's deep-rooted gender disparities contribute significantly to cybercrime against women. Misogynistic attitudes and patriarchal norms perpetuate a culture that allows such crimes to flourish.[21] Women, often seen as easy targets, are subjected to online harassment, abuse, and exploitation with alarming frequency.

(b) Digital Divide

The digital divide in India, characterized by unequal access to technology and limited digital literacy, exacerbates the problem.

[19] Salter, Michael, and Thomas Crofts. "Responding to revenge porn: Challenges to online legal impunity." *New views on pornography: Sexuality, politics, and the law* (2015): 233-256.

[20] Breslow, Alyssa. "The Dangers of the Internet and the Sexual Exploitation of Children." Master's thesis, Utica College, 2018.

[21] Ramirez, Antonio, ed. *An Anthology by Modern Legal Authors*. Highbrow Phantom Publishing House, 2021.

Women, particularly in rural areas, often lack the necessary skills to navigate the online world safely.[22] This lack of awareness leaves them vulnerable to cyber threats, as they may not be aware of the necessary safeguards to protect themselves online.

(c) Inadequate Legal Framework

While India has legislation such as the Information Technology Act, 2000 which cover certain aspects of cybercrime, there is a need for more comprehensive laws specifically addressing cybercrime against women.[23] Current laws often fall short in effectively dealing with the ever-evolving nature of cyber threats, leaving women inadequately protected.

7. Impact of Cybercrime on Women

(a) Psychological and Emotional Distress

- **Anxiety, Depression, and PTSD**: Cybercrime, especially harassment and stalking, can lead to severe mental health issues, including anxiety, depression, and post-traumatic stress disorder (PTSD).[24] The constant fear of being watched or harassed can take a significant toll on a woman's mental well-being.
- **Loss of Self-Esteem and Social Isolation**: Victims of cybercrime often experience a loss of self-esteem and may withdraw from social interactions due to the fear of judgment or further

[22] Lavanya, Reganti, and Rajesh Mamilla. "Closing the Digital Divide in India: Ensuring Equal Access to Technology for Women in Business." In *Effective Technology for Gender Equity in Business and Organizations*, pp. 167-194. IGI Global, 2024.

[23] Jaiswal, Kajal. "Effectiveness of cybercrime laws and regulations in India: A critical study." (2022).

[24] Rothman, Emily F., Jackie Sheridan-Johnson, Poulami Maitra, Toby Shulruff, Chad K. Sniffen, and Elizabeth A. Mumford. "Stress, suicidality, post-traumatic stress disorder, emotional distress, and social isolation among US adults experiencing online abuse or harassment." *Violence and gender* 10, no. 3 (2023): 144-152.

harassment.[25] This social isolation can exacerbate feelings of loneliness and depression.

(b) Threats to Personal Safety

- **Fear for Physical Safety Due to Stalking or Online Threats**: The fear that online threats could escalate into real-world violence is a constant concern for victims of cyberstalking and harassment.[26] This fear often leads to changes in behavior, such as avoiding certain places or people, and can significantly impact a woman's quality of life.
- **Invasion of Privacy and Loss of Personal Control**: Cybercrime often involves a significant invasion of privacy, such as the unauthorized sharing of intimate images or the hacking of personal accounts.[27] This loss of control over one's personal information can be deeply unsettling and lead to a sense of helplessness.

(c). Professional and Social Consequences

- **Damage to Reputation and Career Prospects**: Cybercrime can have devastating effects on a woman's professional life.[28] For instance, the non-consensual sharing of explicit content or defamatory comments can damage a woman's reputation, leading to job loss or difficulties in finding employment.
- **Social Stigma and Victim-Blaming**: In many cases, victims of cybercrime face social stigma and victim-blaming. Instead of

[25] Woods, Naomi. "Users' psychopathologies: Impact on cybercrime vulnerabilities and cybersecurity behavior." In *Cyber Security: Critical Infrastructure Protection*, pp. 93-134. Cham: Springer International Publishing, 2022.

[26] Curtis, Laura F. "Virtual vs. reality: An examination of the nature of stalking and cyberstalking." PhD diss., San Diego State University, 2012.

[27] Ahmad, Mohd Riyaz. "Safeguarding personal privancy in digital era: a study on the right to privacy." (2022).

[28] Agarwal, Dr Pukhraj. "Cyber Crime: Women Combating with the Negative Effect of Technology in the Era of Globalisation." *International Journal of Management and Humanities* 4, no. 7 (2020): 21-25.

holding the perpetrators accountable, society often blames the victims for the abuse they suffer, further compounding their trauma.[29]

8. Addressing the Issue

(a) Awareness and Education

Creating awareness about cyber threats, safe internet practices, and digital literacy is essential to empower women and equip them with the knowledge to protect themselves online. Educational programs aimed at women, particularly in rural areas, can help bridge the digital divide and reduce vulnerability to cybercrime.[30]

(b) Strengthening Legal Frameworks

The government must proactively revise and enhance existing legislation to address the nuances of cybercrime against women. Stricter penalties, faster legal processes, and the establishment of dedicated cybercrime cells are crucial for tackling this issue effectively. There is also a need for more comprehensive laws that specifically address the various forms of cybercrime against women.[31]

(c) Collaboration and Support

Combating cybercrime requires collaboration between government agencies, law enforcement, civil society organizations, and tech companies.[32] Together, they can develop robust reporting mechanisms, provide support to victims, and facilitate the removal of offensive content from online platforms. Public-private

[29] Rackley, Erika, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, and Anastasia Powell. “Seeking justice and redress for victim-survivors of image-based sexual abuse.” *Feminist Legal Studies* 29, no. 3 (2021): 293-322.

[30] Venter, Isabella M., Rénette J. Blignaut, Karen Renaud, and M. Anja Venter. “Cyber security education is as essential as “the three R’s”.” *Heliyon* 5, no. 12 (2019).

[31] Saroj, Vinod Kumar, and Nisikant Nayak. “Investigating Cyber Violence and Harassment Against Women: Challenges and Solutions in the Digital Age.” *Available at SSRN 4900092* (2024).

[32] Tropina, Tatiana. “Cyber-policing: the role of the police in fighting cybercrime.” *Special Issue 2 Eur. Police Sci. & Res. Bull.* (2017): 287.

partnerships can play a vital role in enhancing cybersecurity and protecting women from online threats.

9. Landmark Judgments on Cybercrime against Women in India

The judiciary in India has been instrumental in addressing cybercrime against women, evolving jurisprudence to adapt to the rapidly changing digital landscape. Through landmark judgments, the courts have highlighted the importance of safeguarding women's rights in cyberspace, interpreting existing laws to ensure justice, and filling legislative gaps through judicial innovation.

(a) Recognition of Women's Privacy in Cyberspace

Judgments: Cases like *K.S. Puttaswamy v. Union of India*,[33] and *Nipun Saxena v. Union of India*,[34] have emphasized the constitutional right to privacy, particularly in cases where women's images or data are shared online without consent. The judiciary has recognized that non-consensual dissemination of explicit content infringes on a woman's right to dignity and privacy, mandating stricter enforcement of laws like Sections 67 and 67A of the Information Technology Act, 2000.

Impact: These judgments have led to a broader understanding of digital privacy and the necessity of proactive measures to protect women from cyber exploitation.

(b) Clarifying the Scope of Cybercrime Laws

Judgment: In *Shreya Singhal v. Union of India* (2015),[35] the Supreme Court struck down Section 66A of the IT Act for being vague and overbroad but emphasized the need for clearer and more precise legal provisions to address online harassment effectively.

[33] (2017) 10 SCC 1.

[34] 2019 (2) SCC 703.

[35] AIR 2015 SC 1523.

Impact: This judgment set a precedent for balancing free speech and protection from abuse, urging lawmakers to design specific legislation to combat online gender-based violence.

(c) Setting Precedents for Consent in Digital Spaces

Judgment: The *Indira Jaising v. Supreme Court of India*,[36] ruling underscored the importance of consent in sharing intimate images, holding that such acts without consent constitute a grave violation of dignity and privacy.

Impact: The judiciary reinforced that sharing explicit content without permission should be prosecuted under IPC sections such as 354C (voyeurism) and 509 (insulting modesty), alongside IT Act provisions.

(d) Protecting Women from Morphing and Cyberstalking

Judgment: In *Nipun Saxena v. Union of India*,[37] the Court tackled the issue of morphing and unauthorized dissemination of women's images, treating these acts as severe violations of women's rights to dignity and privacy.

Impact: The judgment emphasized the necessity of stringent penalties and immediate action against offenders, pushing for the establishment of dedicated cybercrime units.

(e) Judicial Directions to Strengthen Law Enforcement

Courts have repeatedly directed law enforcement agencies to adopt a victim-sensitive approach while handling cases of cybercrime against women. Directions include establishment of special cybercrime cells; providing special training to the police and judiciary in dealing with cybercrime-related offences; and accelerate the disposal of cases involving digital evidence.

[36] (2017) 9 SCC 766.
[37] 2019 (2) SCC 703.

(f) Judiciary as a Catalyst for Policy Changes

The judiciary has often acted as a catalyst, urging legislative and executive branches to address gaps in the legal framework. Recommendations from cases like *Subramanian Swamy v. Union of India*,[38] have influenced policy discourse on comprehensive cybersecurity laws tailored to protect women.

10. Conclusion and Suggestions

Cybercrime against women in India is a multifaceted challenge that requires urgent attention and comprehensive solutions. While the rapid expansion of digital platforms offers women opportunities, it also exposes them to new threats in the form of harassment, cyberstalking, identity theft and the non-consensual distribution of intimate content. Despite legal frameworks such as the Information Technology Act 2000 and pioneering judicial interventions, enforcement challenges and loopholes remain, leaving women with inadequate protection.

The judiciary has played a critical role in advancing digital rights, particularly for women, by recognizing privacy as a fundamental right, setting precedents for consent in cyberspace, and pushing for stronger enforcement mechanisms. However, these measures alone are not enough. Effective collaboration between government, judiciary, law enforcement, technology companies and civil society is critical to combating this threat. By focusing on education, legal reform and technological innovation, we can work towards a safer and more inclusive digital environment for women. The following suggestions are recommended:

(a) Strengthening Legal Frameworks

It is necessary to amend the Information Technology Act of 2000 to address emerging threats, such as deepfakes, AI-driven harassment, and cyber grooming. There is a need to enact special laws that focus exclusively on cybercrimes against women and impose strict punishments for crimes such as revenge pornography, cyberstalking, and online trafficking.

[38] AIR 2016 SC 2728.

(b) Judicial Innovations

Need to establish fast-track courts for cybercrime cases involving women to ensure timely justice. Further, Development of policies for handling digital evidence, including mandatory training for judges and prosecutors on cyber laws and digital forensics.

(c) Law Enforcement Reforms

It is necessary to establish specialized cybercrime units focused on combating crimes against women and ensuring the presence of trained female officers, and also to conduct regular training programs for police officers on victim-sensitive handling of cybercrime cases.

(d) Collaboration with Technology Platforms

Mechanisms should be in place to require technology companies and social media platforms to proactively monitor and remove abusive content aimed at women. There is a need to develop automated reporting systems to help victims flag harmful content and access support services.

(e) Awareness and Digital Literacy

High time to launch nationwide digital literacy campaigns targeting women, particularly in rural areas, to educate them about online safety, privacy controls and reporting mechanisms. It is necessary to integrate digital security and cybercrime awareness modules into school and college curricula.

(f) Victim Support Mechanisms

It is important to establish support hotlines and counseling services for cybercrime victims staffed by trained professionals, also to create a centralized online cybercrime reporting portal with multilingual support and streamlined processes.

(g) Public-Private Partnerships

Necessary to collaborate with private organizations and NGOs to conduct workshops on digital security and cybersecurity, and to promote innovation in cybersecurity tools that can detect and prevent cybercrimes against women.

(h) Monitoring and Accountability

The Central Government should establish a national cybercrime regulator to regularly review the effectiveness of laws and policies, and conduct regular audits of law enforcement agencies to ensure accountability in the handling of cybercrime cases involving women.

(i) International Cooperation

The Government should collaborate with global cybersecurity authorities to combat cross-border cybercrime and share best practices, and advocate for international treaties to combat gender-based cybercrime.

By implementing these measures, India can make significant progress in curbing cybercrimes against women and creating a digital ecosystem that ensures security, equality and dignity for all.