International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybercrime Against Women in India

Deepika Muthukumar

I Year BBA., LL.B. (Hons.), Sastra Deemed to Be University

Abstract

Cybercrime in India have become one of the biggest issues in recent times especially when we are in the era where people post their day-to-day activities from their morning coffee to their dinner. The most disturbing cybercrimes though are often against women. Crimes in general, against women are increasing day by day but the most traumatizing crime against women would be cyber-crime. Cybercrimes are not only crimes that were once done physically but now online like eve-teasing, bullying, harassment and blackmail but they have gone to extreme level like hacking of personal data, cyber pornography, cybersex trafficking, cyber sexual defamation and morphing being the most frightening cybercrime of them all. This research paper aims to explain how several types of cybercrime against women in India are increasing at an alarming rate and how well the legal systems work to protect women against them. This research paper will include various reputed cases that made a huge impact in making laws for Cybercrime against women Utilizing a qualitative approach, the article examines key legislation, including the Information Technology Act[1] and relevant provisions of the BNSS[2], alongside an analysis of real-life case studies.

Keywords: Cybercrimes, women, legal provisions

Introduction

In recent times, the digital outlook in India has expanded rapidly, which provides a lot of opportunities for communication, education, and commerce. However, this growth has also been accompanied by a huge growth in cybercrime, particularly against women. The anonymity and reach of the internet create grounds for various forms of harassment, exploitation, and abuse, targeting women in alarming numbers. From online stalking and harassment to identity theft[3] and cyberbullying, women face a lot of threats that can have devastating psychological, social, and economic consequences.

To get an understanding of how dangerous cybercrime is we need to get a better understanding of what cybercrime is "Cybercrime is a criminal activity that either targets or uses a computer, a computer network or a networked device against others"[4].

Even while the number of these offenses is rising, many women are still ignorant of their legal rights and protections. This essay aims to investigate the complicated landscape of cybercrime against women in India, analysing how effective present legislative protections are and identifying significant gaps that must be addressed. Through the presentation of actual situations, the conversation will underscore the pressing

[1] Information Technology Act, 2000 (IT Act): The IT Act is the primary law governing cybercrimes in India, specifically addressing electronic commerce, digital signatures, and cybercrimes.
[2] BNSS: Bharatiya Nagarik Suraksha Sanhita
[3] Definition of IDENTITY THEFT (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/identity%20theft
[4] https://cybercrime.gov.in

need for comprehensive changes and educational programs. The goal of this analysis is to advance knowledge about how to give Indian women a safer online environment so they can move throughout the internet with assurance and security.

Whether in the past or the present there has always been crime against women the only thing that differentiates both is the platform used to commit these crimes against women. physical Crimes against women like eve teasing, abusing, harassment, black mailing, bullying, modesty are now committed thru the cyberspace.

Early in the 1990s, cybercrime started to emerge. Following India's opening to the global digital economy in the 1990s, internet usage became widely prevalent in the country. The legal structure for dealing with cybercrimes was essentially non-existent during this time, and the internet was mainly unregulated. The expansion of the internet into both urban and rural regions led to the rise of online crimes, such as harassment. Urban women were more likely to be victims of cybercrime since rural areas had less internet access. When people first started using the internet, cybercrimes including impersonation, improper content, and email harassment were not common. However, instances of cyberbullying and harassment[5] were beginning to be observed in certain circles, especially affecting women who were more visible online. In the 2000s, women started utilizing technology more frequently as mobile phones and the internet became more widely available. However, as internet usage increased, so did cybercrimes like defamation[6], harassment, and stalking[7]. Online harassment can take many different forms in the 2000s, including uploading libelous[8] content, sending threatening or pornographic emails, and stalking on social networking platform.

Since social media sites like Facebook, Instagram, and Twitter have become more popular, cybercrimes against women have significantly escalated.

With the emergence of social media platforms like Facebook, Instagram and twitter increased cyber-crimes against women increased rapidly. The occurrence of stalking, bullying, and defamation began to surface more prominently. Even Though, The Information Technology Act 2000 [9]was introduced and was a huge step against cybercrime but the scope of protection for women was very limited. In the 2010s, the Indian government and judiciary began to realize the severity of cybercrimes, including those targeting women. The increasing number of reported cases led to the development of legal frameworks to specifically address crimes like cyberstalking, online harassment, and identity theft. With technical advancements and greater digital penetration resulting in an increase in online abuse, harassment, and exploitation, the current state of cybercrime against women in India indicates an increasing concern. As of recent years, cybercrime has gotten more complex, and while there have been considerable advancements in awareness, legal protection, and enforcement, many issues remain. Cyberbullying[10], a type of harassment or bullying carried out using electronic or communication means such a computer, laptop, mobile phone, etc., is one

[5] Definition of HARASSMENT (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/harassment

[6] Definition of DEFAMATION (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/defamation

[7] Definition of STALKING (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/stalking

[8] Definition of LIBELOUS (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/libelousfi

[9] Information Technology Act, 2000 (IT Act): The IT Act is the primary law governing cybercrimes in India, specifically addressing electronic commerce, digital signatures, and cybercrimes.

[10] Under section 499 as per IPC

type of cybercrime. The types of cybercrimes against women have diversified, as new technologies and social media platforms have become more pervasive. Some of the most common forms of online abuse against women in India today include cyberstalking and Online Harassment[11]: Women face repeated unwanted attention, threats, or intimidation through online platforms. This covers threatening messages, stalking on social media, and slander or disparaging comments. One of the most often reported topics is revenge porn and non-consensual pornography. In order to harass, degrade, or threaten women, the perpetrator frequently posts private photos or videos of them without getting their permission. Even though this behaviour is illegal, it is nonetheless becoming more and more common. Sexual harassment on social media: Women continue to encounter unwelcome advances, sexual remarks, and even explicit photos on social media sites including Instagram, Facebook, Snapchat, WhatsApp, and Twitter. These networks' anonymity promotes criminals, making it more difficult for law enforcement to find them. Phishing and identification Theft[12]: Cybercriminals also target women in their efforts to steal identification information, bank account information, and personal data. This can include fraudulent e-commerce transactions, phony lottery winnings, or phony job offers. Doxing[13] and Trolling[14]: Public figures, journalists, activists, and even ordinary women face cyberbullying, which includes the posting of personal information (address, phone number, private images) online with malicious intent. This has been especially true for women who speak out on social issues. Deepfakes and AI-Based Exploitation: A serious problem is the use of AI technologies to produce deepfakes or altered photos and videos in order to harass or disparage women. With the use of these technologies, criminals can create explicit material about women that is identical to authentic photos or films, which they can then use to threaten or harm the victims' reputations.

Objective of the study

The aim of this study is to understand how often cybercrimes happen to women in India, what kinds of online crimes they face, and how these crimes affect them. It will look at the challenges women face in getting justice, including problems with the law, technology, and social support. The study will also review whether current laws and policies are effective in protecting women from online harm. By looking into these topics, the study intends to show how cybercrime affects women in real life and offer solutions for better protecting and assisting them.

Review of literature

According to Sanjeev Kumar[15], the increasing rate of cybercrimes against women can be attributed to two main factors: legal and sociological reasons. Legally, it is evident that the existing laws addressing cybercrime do not explicitly cover these offenses under relevant sections, even though other laws such as the Indian Penal Code (IPC) and the Constitution offer special protection to women. However, the specific regulations concerning cybercrime do not fully reflect this protection. For a variety of reasons, including the victim's hesitancy, shyness, and concern of harming her family's reputation, many cybercrimes against

[11] Under section 354 (D), 509 IPC, and section 67

[12] Sections 66, 66A and 66D of Information Technology Act 2000 and Section 420, 379, 468 and 471 of India Penal Code, 186056.

[13] The act of publicly providing personally identifiable information about an individual or organization, usually via the Internet and without their consent.

[14] under section 354 (D) and 509 of the IPC, and section 67 of the IT Act, section 67 and 67A of the IT Amendment Act 2008.

[15] CYBER CRIME AGAINST WOMEN: RIGHT TO PRIVACY AND OTHER ISSUES October 2019 https://www.researchgate.net/publication/344153821_CYBER_CRIME_AGAINST_WOMEN_RIGHT_TO_PRIVACY_AND_OTHER_ISSUES

women go undetected. Victims are frequently discouraged from pursuing justice because they believe they bear some responsibility for the crimes against them.

According to Mr. Harish Yadav, the prevalence of cybercrimes against women in Indian society is also significantly influenced by patriarchal ideas. A culture of misogyny, victim-blaming, and presumptions is fostered by the patriarchal system, which upholds male supremacy and power. These deeply rooted beliefs frequently carry over into the internet space, where women are subjected to abuse, trolling, and harassment. When women voice their opposition to violence or harassment, they are frequently accused with bringing shame to their towns or families. The absence of family and social support could prevent women from reporting cybercrimes and seeking legal action.

Ms. Saumya Uma[16] similarly states, many women in India are unaware of their legal rights regarding cybercrimes, making awareness-raising a crucial agenda for the government. Women's rights education is crucial for both preventing and dealing with these kinds of crimes. Raising awareness of the laws and viewpoints surrounding cybercrimes against women among the major players in the criminal justice system such as the police, investigating officers, public prosecutors, and judges is equally crucial. Furthermore, developing confidence-building mechanisms for victims and potential victims is critical to encourage them to report crimes. Additionally, grievance redressal mechanisms and institutions should be strengthened and made more accessible, with the main goals being the ease of lodging complaints and minimizing delays in investigation and prosecution.

Legal Framework

India has significantly advanced its institutional and legislative structures to combat cybercrimes against women, and they are. The Information Technology Act of 2000 Section 66E: Deals with invasions of privacy[17], such as taking and disseminating pictures of someone's intimate area without permission. Pornographic[18] content shared without consent is one example of the obscene material that is punishable under Section 67 for publication or transmission in electronic form. Particularly addressing the publication or transmission of sexually explicit actions, Section 67A imposes more severe penalties for such offenses. Targeting child pornography, Section 67B prohibits the publication or transmission of any content that shows children in a sexual way. Section 354D of the Indian Penal Code (IPC) makes stalking, including cyberstalking, a crime. It includes instances in which a guy persistently follows or makes contact with a woman in an attempt to promote intimate relations without her will. Defamation is covered under Sections 499 and 500, which apply when women's reputations are harmed by false claims posted about them online. Criminal intimidation, which includes threats made online, is covered under Section 503. The 2013 Criminal Law (Amendment) Act: By strengthening the punishments for sexual offenses and acknowledging the seriousness of online harassment and stalking, this amendment brought about modifications to several sections of the IPC. The 2013 Act on the Prevention[19], Prohibition[20], and

[16] OUTLAWING CYBER CRIMES AGAINST WOMEN IN INDIA Bharati Law Review, April – June 2017 https://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf

[17] Definition of PRIVACY (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/privacy

[18] Definition of PORNOGRAPIC (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/pornographic

[19] Definition of PREVENTION (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/prevention

[20] Definition of PROHIBITION (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/prohibition

Redress[21] of Sexual Harassment of Women at Work: This regulation can be applied to online harassment in a professional setting, even though its primary focus is workplace harassment. supplying women with channels for reporting and pursuing remedies. The admissibility of electronic documents as evidence is made possible by amendments to the Indian Evidence Act, 1872, which is essential for the prosecution of cybercrimes. The Indian Evidence Act, 1872: Amendments allow electronic Right Act, 1957: Section 63B of Copy Right Act, 1957 provides protection to women from Data Theft. This section provides that any person who knowingly makes use of a computer or an infringing copy of a computer program shall be punishable. Protection of Children from Sexual Offences (POCSO) Act, 2012: POCSO Act, 2012 provides protection to girl child, the provisions are- Section 3 for Penetrative Sexual Assault, Section 5 for Aggravated Penetrative Sexual Assault, Section 7for Sexual Assault, Section 9 for Aggravated Sexual Assault, Section 11 for Sexual Harassment of the Child, Section 13 for Use of Child for Pornographic Purposes. The constitution of India guarantees equal right to life, right to live with human dignity and right to speech and expression to women but the same modesty of women seems not to be protected in general in the Information Technology Act, 2000.

Conceptual Framework

The case of Ranjeet D. Udeshi v. State of Maharashtra [22]is a significant cybercrime case in India related to the sending of obscene material through the internet. This case highlighted issues of cyber obscenity, online harassment, and the legal interpretation of indecent or offensive content shared electronically. His name was Benjamin Franklin and after his name the test was named as Hicklin Test[23]. Basically, it is an obscenity standard that originated in an English case- Regina vs. Hicklin (1868)[24], this case is based on women pornography and obscenity which was decided by the Court of Queen's Bench in the UK, in this case a propounded doctrine named Hicklin test is a standard of obscenity in context of women pornography. The definition A work is obscene if it tends to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall. under the Hicklin Test, the focus was on whether any portion of the material could tend to corrupt or deprave a vulnerable segment of the population, particularly those who were more vulnerable to such influences, such as children or the impressionable. Shreya Singhal v. Union of India (2015)[25] – Section 66A of the IT Act Shreya Singhal, a law student, challenged Section 66A of the IT Act after two women were arrested for posting a Facebook message criticizing the shutdown of Mumbai on the death of a political leader. Because they reportedly sent abusive words online, the police arrested them under Section 66A. In 2015, the Supreme Court of India ruled that Section 66A of the IT Act was unconstitutional, citing a violation of Article 19(1)(a) of the Constitution's basic right to free speech. According to the Court, the provision was vague and overly broad, which encouraged abuse and unjustified imprisonments. Although this ruling was viewed as a win for online freedom of speech, it also sparked debate about the need for stricter legislation to shield women from harassment online. Nikhil Soni v. Union of India (2020): Online harassment and cyberbullying in this instance, a woman named Nikhil Soni complained about being harassed online on

[21] Definition of REDRESS (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/redress
[22] Ranjit D Udeshi v. State of Maharashtra 1965 AIR 881
[23] The Hicklin test is a legal test for obscenity established by the English case R. v Hicklin.
[24] England and Wales High Court of Justice, Queen's Bench Division 11 Cox C.C. 19 (1868)
[25] Shreya Singhal v union of India air 2015 SC1523

several social networking sites. She alleged that a group of people were bullying and spreading hateful content against her, damaging her reputation. The Rajasthan High Court ruled in favour of the petitioner and directed police authorities to take swift action against the cyberbullying. It brought attention to the necessity of stricter social media platform regulations in order to stop harassment. Suresh N. v. State of Maharashtra (2019): Defamation and Cyberstalking. A man from Maharashtra named Suresh N. was charged with defamatory posts on social media and cyberstalking a woman. The woman claimed that Suresh had caused her great mental anguish and harm to her reputation by making fake profiles and spreading untrue data about her. The accused was found guilty by the court under several sections of the Indian Penal Code (IPC), such as Section 66E of the IT Act (privacy violation), Section 500 (defamation), and Section 354D (stalking).

The legal environment surrounding cybercrimes against women in India has been significantly shaped by the court cases covered above.

Key issues

Lack of Awareness and inadequate support systems for women, many women are sadly not aware of their rights regarding cybercrime which prevents them from seeking justice or reporting offenses. Another significant barrier is the lack of awareness about how to report cybercrimes. Women may not know which authorities or organizations to approach when they are victims of online harassment or exploitation[26]. In addition to frequently receiving fewer reports, police and cybercrime units lack adequate outreach activities and awareness campaigns to inform the public about the reporting processes. Women are unable to promptly pursue legal redress due to this lack of knowledge. Women frequently might not even be aware that there are specialist cybercrime cells or helplines for dealing with internet offenses. For example, the National Cyber Crime Reporting Portal[27] was set up to allow people to report cybercrimes, but many victims remain unaware of this resource. The National Commission for Women[28] (NCW) is also one of statutory body that plays a key role in protecting women's rights in India. Social Stigma: Societal attitudes often discourage women from reporting cyberstalking due to fear of victim-blaming or stigma, which undermines the effectiveness of existing laws. In India's patriarchal society, women often face social stigma when they are victimized, particularly when the cybercrime involves sexual harassment or the sharing of intimate content. Victims may feel embarrassed or ashamed to come forward, especially if they fear they will be blamed for the crime or accused of bringing shame to their family or community. Because of this fear, women may keep quiet and put up with abuse without getting the support or legal protection they are entitled to. How can a woman in India, where society frequently places blame on women, come out and file a case when her dignity or reputation is endangered? Another important factor preventing women from reporting cybercrimes or pursuing legal action is cultural and societal standards. Family members or peers frequently advise women who are the targets of cybercrimes to ignore the harassment or move on from the event. Such suggestion is the result of deeply rooted patriarchal beliefs that minimize the gravity of the offense and discourage women from openly addressing it.

[26] Definition of EXPLOITATION (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/exploitation
[27] DEFNITIONS OF CYBERCRIME - https://cybercrime.gov.in/
[28] National commission for women - http://ncw.nic.in/

Evolving Technology: With the growth of the internet, Women are more vulnerable to a variety of cybercrimes that take use of modern technology thanks to social media platforms and mobile devices. such as social media, which made online bullying, harassment, and trolling more widespread. These sites give criminals the anonymity they need to attack women.

Solutions and Recommendations

Regarding the lack of awareness among women, initiatives such as Public Awareness Campaigns should be launched by the government and non-governmental organizations to educate women about cybercrimes, their rights, and the legal protections that are available to them. These campaigns should be accessible, relatable, and understandable to women from a variety of locations, including different age groups, educational backgrounds, and geographical areas. Programs aimed at enhancing digital literacy should be put into place, particularly in rural and underprivileged areas, to help women understand the risks of using the internet and give them the tools they need to defend their online presence from cyber threats[29]. In the case of lack of awareness about how to report cybercrimes, creating easily accessible helplines, websites, and mobile apps where women can report cybercrimes without fear of judgment is crucial. These resources should be widely advertised and available in multiple languages where the women can use them easily.

In the case of social stigma, awareness to the public in highly important so that the society understands the extent of cybercrime against women and how cruel they are.

Conclusion

Women's safety and dignity are at risk in the internet world because to the rising and complex problem of cybercrime against them. The strategies employed by cybercriminals also change with technology, making it more challenging to stop these crimes. Cyberstalking, revenge porn, identity theft, and cyberbullying are just a few of the many types of online harassment that have a significant impact on women. In addition to the psychological and emotional trauma[30] caused by these crimes, women frequently experience victim-blaming and social stigma, which deters them from reporting cybercrimes. Even if laws like the Information Technology Act of 2000 have made some progress in combating cybercrimes, there is still a long way to go before women are adequately protected online. Victims[31] are frequently left defenceless and reluctant to disclose the abuse they endure due to a lack of knowledge about their legal rights and a weak support network.

In parallel, cultural change is essential to challenge the patriarchal attitudes that perpetuate online violence[32] against women. Changing the mindset of the society is the key to encouraging more women to report cybercrimes. Once the victim blaming comes to a halt women will be more confident in reporting such crimes.

[29] Definition of THREAT (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/threats

[30] Definition of TRAUMA (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/trauma

[31] Definition of VICTIM (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/victims

[32] Definition of VIOLENCE (Merriam-Webster: America' s Most Trusted Dictionary) https://www.merriam-webster.com/dictionary/violence

In the end preventing and addressing cybercrimes against women requires societal change as well the mass awareness about their rights only then can we ensure a safer and more equitable online world for women.