Research Reinforcement | A Peer Reviewed International Refereed Journal | ISSN 2348-3857
Vol. 10, Issue 2 | November 2022 - April 2023 | pp. 134-138

Women's Susceptibility to Cyber-Sexual Assault: Prevention and Treatment

Dr. Parul Pareek

Legal Associate, Former Assistant Professor Sol,
Mody University of Science and Technology, Laxmangarh, Sikar (Rajasthan)

Abstract

The prevalence of gender-based violence has changed as a result of the development of digital and communication technologies and the globalisation of Internet access. It has been established that the influence of these two factors increased internet accessibility. The number of uncommon forms of violence against women that have been documented has dramatically increased in recent years. It is conceivable for crimes against women to be conducted utilising digital and technologically based methods, utilising a wide array of platforms and technology, including, among other potential instances, video games and software for video conferencing. These offences can be committed using digital and technological tools. Even though incidents of legal violations are frequent throughout a range of legal arena, it is typical for intermediaries and wrongdoers to not be held accountable or culpable for their actions. This article examines the difficult issue of sexual assaults against women that take place online, concentrating on the elements that make women more vulnerable to such assaults and the potential solutions to the issue that these assaults raise.

Keywords: *Women, Sexual Assault, Crime, Cyberspace*

Introduction

The issue of "cyber sexual assault" against women in India has been largely overlooked and inadequately addressed, resulting in a state of vulnerability for the affected victims. The prevalence of digital technologies and global Internet access has resulted in a shift in the nature of crimes committed against women and girls. The swift proliferation of cyberspace has given rise to novel forms of aggression. The emergence of mobile devices, social media, and other forms of communication technology has given rise to novel avenues for gender-based violence. The widespread availability of digital content and the ability to leave a digital footprint have compounded the negative impact on victims at the individual, community, and societal levels. Crimes against women that are facilitated by internet and technology are observed across multiple platforms and technologies, including social media networks, private messaging applications, email services, dating applications, forums, video games, and videoconferencing platforms. The recurrence of victimisation is a common phenomenon due to the public visibility and open communication of the violence. The perpetration of these crimes is a common occurrence across multiple jurisdictions, without taking into account the responsibility of intermediaries and perpetrators. The perpetration of cybercrimes against women via online platforms and emerging technologies has significant implications for various facets of the victims' existence, including their personal and familial well-being, physical and mental health,

economic sustenance, social standing, and other related domains.

Types of Serious Crimes Committed Online Against Women

In addition to the category of gender-neutral crimes, following are some of the most significant cyber-based sexual assaults[1] against women that have emerged in recent years[2]:

Cyber Stalking: It's one of the most discussed and perpetrated cybercrimes nowadays. Stalking involves following the victim over the Internet by posting remarks or threats on bulletin boards, entering chat rooms, and flooding the victim with emails, messages, etc. According to a Norton by Symantec survey, 63% of respondents reported abuse and insults against women in cyberspace, followed by rumormongering (59%), posting malicious comments/threats on social media (54%), trolling (50%), and orchestrated coordinated group attacks (49%).[3]

Sextortion and Cyber Defamation: The act of extorting individuals for financial gain or sexual favors through the use of electronic communication technologies is a prevalent form of cybercrime. The individual who engages in extortion employs the tactic of leveraging the threat of disseminating photographs, videos, or personal information unless the victim provides monetary compensation or engages in further sexual activity. The prevalence of sextortion cases is increasing on a daily basis in India, with a staggering number of over 700 million smartphone users in the country.[4]

Morphing and Cyber Obscenity: The term "morphing" pertains to the act of altering an individual's image derived from their personal online photographs or self-captured photographs through the utilization of computer software. Free smartphone applications that are readily available on the play store can be utilized for basic morphing. These applications are frequently employed to produce indecent images of women, wherein certain components of the image are altered and overlaid with another indecent image. In addition to the widely disseminated fake photograph, the perpetrator may also engage in the posting of vulgar language on the victim's social media profile. Modifying the original photographs of a female victim on her profile through unauthorized access is a type of cyber sexual assault. The act of utilizing the modified photos and the user's identity to disseminate derogatory messages via email to the user's acquaintances, as well as sharing them on the internet, is observed.

Cyber Bullying and Trolling: The phenomenon of gender-based cyberbullying and trolling in India has received limited scholarly attention. India exhibits the highest gender disparity[5] in mobile phone and Internet access (46%) among South Asian countries. In India, there is a significant gender disparity in cell phone ownership, with 79% of men possessing cell phones in contrast to 43% of women. Based on estimations, a mere 24% of women in India possess smartphones, while a mere 11% have access to the Internet. According to a survey[6] conducted in 2017 in Tier-1 Indian cities, it was found that a significant proportion of respondents, who are presumably well-educated and informed, reported experiencing online harassment. Specifically, 80% of the respondents reported facing online harassment, while 41% of women reported experiencing online sexual harassment.

Cybersex Trafficking: The act of cybersex trafficking involves the perpetrator broadcasting, recording, or disseminating visual content depicting the victim engaging in intimate or personal activities from a centralized location. The aforementioned material is advertised and sold through online platforms to individuals who engage in sexual predation and procurement. The individual in question has allegedly been subjected to blackmail and coercion, resulting in their involvement in the commission of the aforementioned crime.

Girl Child Grooming: Perpetrators who aim to exploit a juvenile female for the purposes of cybersex or pornography will initially establish a friendly relationship and cultivate a sense of confidence with her. Perpetrators in such situations frequently establish intimate connections with

their targets due to their extensive knowledge of their lives and the lives of the minors they exploit. Subsequently, the perpetrator initiates the process of pressuring the minor into engaging in sexual activities, and due to the child's apprehension and embarrassment, it becomes exceedingly challenging for them to extricate themselves from the perpetrator's abusive grasp.

Revenge Porn: In the event of a relationship dissolution between a male and female, the former partner, specifically the ex-boyfriend or ex-husband, may engage in the unauthorized dissemination of intimate visual media content, including photographs or videos, to the intended recipient and/or other individuals. The term "Vengeance Porn" pertains to this phenomenon. The terminology in question is not explicitly employed within the provisions of the Information Technology Act of 2008. Research indicates that the majority of victims of revenge pornography, up to 90%, are female. The perpetrators experience minimal or negligible consequences. On the contrary, it fosters a culture of victim-blaming and may result in a decreased incidence of crime reporting.

Virtual rape: The aforementioned phenomenon refers to a type of cyber victimization that involves the use of violence, albeit non-physical, against a female target. The individual responsible may engage in persistent communication that includes explicit threats of sexual violence, or alternatively, the victim may be subjected to a collective assault that has been incited by such rhetoric. Breaking the cycle of online sexual assaults can prove to be an arduous task for the victim, as she becomes a subject of salacious discourse and indecent language. With the advent of the Metaverse, a digital realm featuring virtual representations of individuals, instances of sexual harassment and rape perpetrated against women in this space are becoming increasingly prevalent.

Factors Contributing to Women's Vulnerability in Cyberspace

Women's internet vulnerability can be explored in two parts[7]:

A. Legal Factor: The IT Act, 2008 was designed to boost e-commerce. So, it covers commercial or economic crimes like hacking, fraud, violation of confidentiality, etc., but the drafters probably didn't consider Internet user safety. Apart than e-commerce-related offences, Sections 66 (hacking), 67 (publishing or distributing obscene content in electronic form), and 72 (breach of confidentiality) of the Act cover most cybercrimes. Internet defamation, email spoofing, cybersex grooming, virtual rape, porn vengeance, cyber stalking, etc. are not covered under the IT Act. India was one of the few countries to pass the IT Act in 2000 to tackle cybercrime, but women's issues were left out. The Act punishes hacking and publishing obscene material online, but the typical cybercrimes against women discussed above are not. The Indian Penal Code, Criminal Procedure Code, and Constitution protect women. Online offences against women were not particularly penalised until recently. After the 2012 Delhi Gang Rape case, there was a strong call for new legislation and penalties to protect women from sexual offences and speed up justice. The Criminal Law Amendment Act 2013 added sections 354, 354, A, B, C, and D to the Indian Penal Code. Today, these divisions address pornography, morphing, slander, etc. Cybercrimes are rising due to the Internet's fluidity. Section 75 of the IT Act, 2008 covers offences committed outside India, although it does not address cybercrimes. The IT Act does not prohibit cyberpornography. Cyber pornography is usually a bailable offence under section 66 E. As bail is simple, offenders repeat pornography-related offences. Compounding causes include the lengthy trial and lack of rapid victim relief. These legal loopholes enable criminals, who operate without fear. Section 67 of the IT Act only punishes transmission and publication, not viewing and downloading, making it impossible to monitor obscene materials online. Sections 66 and 67, which are utilised for cybercrimes, only provide a 3-year sentence, which is not deterrent.

B. Sociological Factor: Cyber sexual offences against women in India reflect oppression and misogyny. Because of this, female crime victims are deterred from seeking justice. Women's

crimes were once limited to roadways and other areas away from home, the safest place on earth. Criminals now lurk in the home and use smart devices and internet platforms to steal private information. Most women don't report cybercrimes because they don't want to embarrass their families. If they find out, family members discourage the victim from reporting the crime. Since the offender is usually unidentified, there is a danger of ongoing threats and blackmail. Women victims often think reporting the incident will make their family life worse.[8] They also worry about whether their family and friends will support them and how society would see them. The victim typically believes she committed the crime against her. Women fear reporting crimes, which encourages offenders.

Suggestions

The most significant challenges posed by cybercrime are, without a doubt, its intricacy and persistence. In order to immediately identify the perpetrator and take steps to assist the victims, law enforcement, the judicial system, and investigative agencies need to keep up with improvements in web-based application technology. Following are some suggestions to help prevent crimes committed online against women:

1. Raise awareness in the community about the dangers posed by these sorts of cybercrimes in order to better protect women and children from falling victim to them and safeguard their safety.
2. Students in schools and other educational settings should be taught about legal remedies for cybercrimes as a routine part of the curriculum in order to raise their awareness of these options.
3. Investigative officers at police stations and members of the Cyber Cell should be trained to deal with offences of this nature. Training on a consistent basis should keep their knowledge and abilities updated.
4. Experts in cybercrime ought to be subject to regulation. It is time to start thinking about creating a separate cadre of cyber experts since dealing with digital data and cyberspace is a technically demanding undertaking that requires expertise that some police officers may not have.
5. Victims should be granted anonymity and privacy in order to increase the likelihood that they will come forward to the Legal Enforcement Agency.
6. In order to successfully handle cases, each Cyber Cell needs to have access to the most advanced Cyber Crime Investigative Tools available.
7. Experts in forensics should have the authority to effectively handle digital evidence and provide the Legal Enforcement Agency with advice as promptly as possible.
8. The development of a standard operating process for conducting investigations of online crimes committed against women.
9. The establishment of treatment and therapy facilities specifically geared towards victims of cybercrime.[9]
10. In order to provide accurate information in a timely manner, the process of gathering information must to be speed up in order to make it possible to communicate with Service Providers who are located in other countries.
11. Developing the Indian Response System into something similar to CERT in order to more rapidly remove hazardous content from the internet.
12. The majority of Cybercrimes need to be made non-bailable offences. A comprehensive data protection regime needs to be incorporated into the law to make it effective. The government should work towards bilateral cooperation with other countries for exchanging information on Cyber Law.

Conclusion

It is abundantly clear that cybercrimes committed against women over the course of years, is steadily rising. Women have long been the victims of numerous crimes that are specifically directed

against women, and now, on top of that, they are also victims of these modern cyber-crimes. The major issue with cybercrime is that it is much more challenging to combat than traditional crime because it transcends state and national boundaries. Additionally, everyone owns one or more electronic devices. Even though the perpetrators are far from the victim, it is still simpler for them to perform cybercrimes. In that situation, girls' and women's self-awareness is also crucial in order to prevent themselves from making themselves into a victim. Women are extremely underinformed about cyber laws and what to do next after becoming a victim of a cybercrime. This causes mental suffering and has frequently prompted victims to try self-harm and related things. Therefore, it is crucial for women to be informed of cyber laws both to prevent becoming victims of such crimes and to report them. Another crucial aspect is that, even today, the investigation process for a cybercrime still uses fairly traditional investigative techniques. Because there are new types of crime, there must also be new means to combat then. The government and other authorised authorities and organisations must step up their efforts to improve cyber security. Cyber patrolling, awareness, training, and investigator capacity building can all contribute to reducing the threat of cybercrime. Even today, the steps taken after reporting a cyber-crime are crucial.

References

1. Garg, R. (2021). *Everything about cybercrimes against women*. [online] iPleaders. Available at: https://blog.ipleaders.in/everything-about-cyber-crimes-against-women/ [Accessed 28 Apr. 2023].
2. Halder, D. & Jaishankar, K. (2016). *Cyber Crimes against Women in India*. New Delhi. SAGE Publications India.
3. Bhargava, Y. (2017). *8 out of 10 Indians have faced online harassment, The Hindu*. Available at: https://www.thehindu.com/news/national/8-out-of-10-indians-have-faced-online-harassment/article19798215.ece (Accessed: April 28, 2023).
4. Ncrb.gov.in. (2021). *Crime In India | National Crime Records Bureau*. [online]. Available at: https://ncrb.gov.in/en/Crime-in-India-2021 (Accessed: April 28, 2023).
5. Van der Wilk, A. (2021). *Protecting women and girls from violence in the digital age*. [online] Council of Europe Publishing. Available at: https://edoc.coe.int/en/violence-against-women/10686-protecting-women-and-girls-from-violence-in-the-digital-age.html [Accessed 28 Apr. 2023].
6. Ghosh, S. (n.d.). *Decoding Gendered Online Trolling in India*. [online] ORF. Available at: https://www.orfonline.org/expert-speak/decoding-gendered-online-trolling-in-india/.
7. Kothawade, M. & Agarwal, P. (2016). Cybercrimes: An Indian perspective. *International Journal of Engineering Science and Computing*, [online] p.3863. doi:https://doi.org/10.4010/2016.895.
8. Mirani, S., Pannu, P. & Malhotra, C. (2014) "Empowering women through ICTs: Cyber Campaigns on Violence Against Women in India," *Indian Journal of Public Administration*, 60(3), pp. 679-695. Available at: https://doi.org/10.1177/0019556120140325.
9. www.mha.gov.in. (n.d.). *Ministry of Home Affairs | Government of India*. [online] Available at: https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme [Accessed 28 Apr. 2023].