Cyber Security's Role in Preventing Crimes Against Women

***Dr. Ravi Bala Goyal**
****Geetansh Goyal**

ABSTRACT:

The freedom to use the internet was recognised as a human right by the United Nations Human Rights Council in 2016. With an emphasis on science and technology for the nation's inclusive development, India has seen a sharp rise in internet users. But as technology has advanced and access to the internet and social media platforms has become more widespread, so too have online crimes against women. The article will examine how technology contributes to the fact that women are more susceptible to cybercrimes than males are. To keep one step ahead of criminals, the court, police force, and investigative agencies must be outfitted with cutting-edge web-based apps. Additionally, the role and responsibility of the government will be discussed, as well as the legal remedies provided by the various cybercrime-related laws. The numerous causes of the rise in cybercrimes against women and how they affect victims will also be a major part of this essay. The study ends by underlining the flaws in the system, where neither the Information Technology Act nor the Indian Penal Code adequately handle such crimes and provide sufficient safety measures. The author(s) will suggest the essential actions to successfully address the problem of cybercrimes against women.

Keywords: Internet users, legislation, cybercrime, and legal remedies are some related terms.

Introduction

India is rapidly growing, largely due to technological advancements. While this progress is commendable, it also poses a downside. Internet users, especially women, are at a higher risk of falling prey to cybercrimes, such as online harassment, hacking, and identity theft, among others. Women are more vulnerable to these crimes due to several reasons, including a lack of privacy safeguards and insufficient awareness about cyber threats.

The United Nations Human Rights Council recognizes internet usage as a fundamental human right. The number of social media users in India has increased significantly, from 181.7 million in 2015 to 250.8 million in 2016, with projections reaching 336.7 million by 2016. However, women constitute only 29% of internet users in India, and they often become victims of cybercrimes, which can have serious consequences.

Despite India being one of the few countries with legislation to combat cybercrimes, special

provisions for crimes against women have not been adequately addressed. Cybercrimes and the objectification of women are increasing worldwide, posing a serious threat to safety and mental health. Cybercrimes such as email spoofing and morphing lack a moral foundation in society and are, therefore, not treated seriously.

A lack of respect for women and interference in their private lives are prevalent issues in contemporary society. To combat cybercrimes against women, individuals must learn to respect each other's rights and understand the nature of crimes. Societal progress is necessary, and young children must be taught to appreciate and respect women from an early age. In addition to stricter laws, changes in the educational system are essential. Cooperation from the public, government, NGOs, and other groups is necessary as no single section of society can bring about this change alone.

Cyber crimes

Any criminal behaviour that uses technology to specifically target women is referred to as cybercrime against women. It may manifest itself in a number of ways, such as sextortion, revenge porn, cyberstalking, and online harassment. Social media, messaging applications, and other digital channels are often used by cybercriminals for their operations. Cybercrime against women may injure them physically, emotionally, and psychologically.

Cybercrime against Women

Various forms of cybercrime against women include:

Cyberstalking is the practise of stalking, harassing, or intimidating women through technology.

Online harassment is the act of sending offensive or threatening messages to women via technology.

Revenge porn is the uninvited dissemination of sexually graphic pictures or films of women.

Sextortion is using technology to pressure women into giving in exchange for cash or sexual favours.

Cybercrime's effect on women

The effects of cybercrime on women's personal and professional life may be serious. The following are some effects of cybercrime against women:

Psychological injury - Cybercrime against women has the potential to seriously impair a victim's mental health, particularly by contributing to despair, anxiety, and PTSD.

Emotional anguish - Women who are the victims of cybercrime may feel violated, degraded, and embarrassed.

Cybercrime may hurt women's professional reputations, which can result in lost employment prospects and career losses.

Stalking, sexual assault, and even murder are examples of how cybercrime may progress into physical violence.

LEGAL PROTECTION (REMEDIES)

The case of Suhas Katti v. State of Tamil Nadu, heard by a Chennai court in 2004, resulted in the country's first-ever conviction for cyberpornography. The defendant, after having his marriage proposal rejected, sent offensive, harassing, and defamatory messages to the victim using a fake email account in her name. The Chennai Cyber Crime Cell was able to secure a conviction under various sections of the Indian Penal Code, resulting in a two-year sentence and a fine for the accused. Similarly, the case of SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra was the first instance of cyberdefamation in India, where the plaintiff sued an employee who had been anonymously sending defamatory emails about the company's managing director to its business partners. With the help of a computer expert, the plaintiff was able to identify the defendant and secure an ad-interim injunction from the Delhi High Court prohibiting further disparaging emails. The courts have played a crucial role in ensuring legal security on the internet, and it is important for people to trust and believe in the judicial system to deliver justice and promote social development.

India has several legal provisions to protect individuals and organizations from cybercrime. The following are some of the main legal safeguards:

The main law controlling cybercrime in India is the Information Technology Act, 2000 (IT Act). It outlines numerous cybercrimes and their punishments, and it gives legal validity to electronic documents, digital signatures, and electronic transactions.

Indian Penal legislation (IPC): The IPC is India's primary criminal legislation and contains a number of sections that may be used to cybercrimes. For instance, cybercriminals may be brought to justice under Sections 408 (criminal breach of trust), 420 (cheating), and 499 (defamation).

The 1872 Indian Evidence Act: Guidelines for the admission of electronic evidence in court are provided under this statute. It describes how digital evidence may be verified and used as proof in court.

Digital media ethics code and intermediary guidelines for information technology, These rules were only recently adopted to control digital media and social media middlemen. They establish guidelines for the removal of harmful material and demand that intermediaries carry out certain due diligence procedures, such as designating a grievance officer.

The Personal Data Protection Act: By establishing rules for the gathering, handling, and storing of personal data, this measure aims to safeguard such data. It also establishes a Data Protection Authority to supervise how the legislation is put into practise.

The Cyber Swachhta Kendra is a government programme that offers residents free tools and services to safeguard their personal computers and mobile devices from online threats.

The National Cyber Crime Reporting Portal is a website where users may submit an anonymous complaint of a cybercrime. The webpage also offers instructions on how to avoid being a victim of cybercrime and how to get assistance.

In general, these legislative safeguards provide a foundation for combating cybercrime in India. To

enhance the judicial system and raise public awareness of the dangers of cybercrime, there is still considerable work to be done.

THE PART OF GOVERNMENT

The Indian government must take a significant part in the fight against cybercrime in the nation. The Indian government has taken a number of actions to strengthen the nation's cybersecurity architecture because it understands how crucial it is to confront the problem of cybercrime. The following are a few government initiatives:

The Information Technology (IT) Act was enacted in 2000 to handle several types of cybercrime in India. In 2008, the legislation was revised to include additional clauses that address cybercrimes such data theft, hacking, and cyberterrorism. In order to address cyber events and advance a safe cyber environment in the nation, the government has formed the Indian Computer Emergency Response Team (CERT-In).

Cells for the investigation of cybercrime: The government has established CICs in several places around the nation. In their respective areas, these units are in charge of analysing and preventing cybercrime.

Awareness Programmes: To inform the public about cybercrime and how to avoid it, the government has started a number of awareness campaigns. A Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been established by the Ministry of Home Affairs to educate Indian internet users about the dangers of cyberattacks.

Foreign Collaboration: To tackle cybercrime, the Indian government has been actively collaborating with foreign authorities and organisations. For the purpose of exchanging knowledge and experience in the field of cybersecurity, the government has signed a number of agreements with nations like the United States, Japan, and the European Union.

Strengthening Cyber Laws: To improve the nation's cybersecurity framework, the government has recently recommended changes to the IT Act. Increased fines for cybercrimes are one aspect of these reforms, and another is the need that international businesses retain user data from India domestically.

THE CURRENT LEGAL SCENARIO'S LOOPHOLES

Through the adoption of the Information Technology Act of 2000 and the creation of a specialised organisation, the Cyber Crime Investigation Cell, to investigate and prosecute cybercrimes, India has made progress in combating this crime. The existing system still has severe flaws, however, which limit how well it can stop cybercrime.

The general public's lack of knowledge about cybercrime and its effects is a significant problem. Many individuals are unaware of the dangers of accessing the internet, such as identity theft, phishing, and other frauds, particularly in rural regions. This leaves them open to cybercriminals who prey on their ignorance to commit crimes.

Another issue is that law enforcement organisations lack the infrastructure and resources necessary to successfully combat cybercrime. Many police agencies lack the technical know-how and resources required to look into and prosecute cybercrimes. In addition, there is a lack of qualified staff in the area of cybercrime, which hinders law enforcement organisations' capacity to properly address the escalating danger.

The lack of coordination and collaboration amongst the many authorities tasked with countering cybercrime is a related problem. The duties of several authorities are sometimes unclear and overlapped, which may cause delays and gaps in the investigation and punishment of cybercrimes.

The difficulty of acquiring evidence in cybercrime cases is another problem, particularly when the offender is based abroad. International collaboration is necessary to investigate and punish cybercrimes, however since various nations have varied cybercrime laws and regulations, it may be challenging to work together and convict cybercriminals.

Finally, because technology and the internet are developing so quickly, cybercrime is also changing and evolving all the time. In order to successfully fight cybercrime, law enforcement authorities and the legal system must keep up with the constant emergence of new kinds of cybercrime.

CONCLUSION

In conclusion, the growing use of technology and social media has led to an increase in cybercrimes against women. There is still considerable work to be done, despite the legal and regulatory actions the Indian government has made to address this problem. Cybersecurity is crucial in avoiding crimes against women online, and practical solutions like encryption, two-factor authentication, anti-malware software, training, and awareness campaigns may help shield women from dangers. In order to guarantee that women are secure and protected in the digital realm, it is critical to continue to address this problem comprehensively.

***Department of Zoology**
Government College
Gangapurcity (Raj.)
****Student**
M.Tech. in Cyber Security,
Sardar Patel University of Police,
Security and Criminal Justice
Jodhpur (Raj.)

REFERENCE

1. Mayura U. Pawar, Archana Sakure .Cyberspace and Women International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 – 8958, Volume-8, Issue-6S3, September

2. Halder D. & Jai Shankar, K. Cyber victimization in India: A baseline survey report. Center for Cyber Victim Counselling Tirunelveli, India. 2010 Available at http://www.cybervictims.org /CCVCresearcher report 2010.pdf (Accessed on 2020.01.11)
3. The Information and Technology Act 2000
4. Press Information Bureau Government of India Ministry of Women and Child Development on 28 DEC 2016 4:33PM by PIB Delhi
5. Dr. Mrs. K. Sita Manikyam, Cyber Crime – Law and Policy perspectives, 40 (Hind Law House, Pune, 2009).
6. Cyber Crimes and the law, Legal India,legalnews and law resource portal, available at http://www.legalidia.com/cyber-crimes-and-the-law/.
7. Dhruti M Kapadia ,Cyber Crimes Against Women And Laws In India , https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/.
8. Id. at 6. v Debarati Halder, Cyber Crime Against Women in India, www.cyberlawtimes.com/articles/103.html. vi Id. at 8.