An Insight into the Cyber Security of Women in India

Dr.Ranjith Somasundaran Chakkambath*, Dr.Shamsi Sukumaran**

*Asst. Professor, Department of Management, Amity Global Business School Kochi, Kerala, India
Email: ranjithsc2016@gmail.com
** Asst. Professor, Department of Management, Amity Global Business School Kochi, Kerala, India
Email:shamsi.kk@gmail.com

--------------------------------------﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡--------------------------------

Abstract:

The incidence of cybercrime has risen in the post-COVID-19 era. Numerous reports from various global regions have highlighted the surge in this domain since the advent of high-speed internet and the digital age. This paper examines the cybersecurity concerns pertaining to women in India, specifically addressing their growing vulnerability and victimization in cybercrimes. The data was collected from different secondary sources including reports, journals and other related articles relevant to the research. There is still lack

*Keywords —*Cyber security, Women, Cybercrimes, Cyber laws, Existing laws in India

--------------------------------------﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡﹡--------------------------------

I. INTRODUCTION

In recent years, there has been an increasing concern about the cybersecurity of women in India. With the rapid growth of technology and internet usage, women in India are becoming more vulnerable to cybercrimes. The lack of awareness and computer literacy among women in India make them easy targets for cybercrimes. Furthermore, societal factors such as gender-based discrimination and patriarchal norms contribute to this vulnerability. As a result, it is crucial to address the causes and impacts of cybercrimes on women in India [11]. The importance of cybersecurity cannot be overstated in safeguarding individuals and entities against diverse cyber threats. It encompasses the preservation of digital information and systems' confidentiality, integrity, and availability. Recently, there has been a heightened focus on addressing specific vulnerabilities and obstacles encountered by women in India within the realm of cybersecurity. As our world becomes increasingly digitized, women in India are more frequently becoming targets for cybercrimes and online harassment. In 2022 alone, the National Commission for Women received nearly thirty-one thousand complaints concerning crimes perpetrated against women—marking the highest number since 2014—as reported by authorities given that case numbers have slightly increased compared to previous years. The majority of these cases were related to the right to live with dignity and followed by domestic violence cases[1]. The number are not showing a positive direction even in this technologically advanced era in India. Women face various forms of cyber threats such as cyber stalking, online harassment, cyberbullying, identity theft, and scams. These cyber threats not only violate the privacy and security of women but also have a significant impact on their mental and emotional well-being. Women in India are considered more vulnerable to cybercrimes due to various societal factors such as gender inequality, patriarchal norms, and lack of awareness about cybersecurity measures [2]. Furthermore, the cyber laws in India provide some protection for women against such cybercrimes.

However, there is a need for further research and initiatives to enhance cybersecurity measures specifically targeted towards the safety of women in India. This research paper aims to examine the cyber security challenges faced by women in India and explore the existing legal provisions and initiatives to combat cybercrimes against women in the country.

1.1 Objectives

The objectives of this research paper are:-

- To identify the different types of cyber threats faced by women in India.

- To identify the existing cyber laws for protecting women in India.

II. LITERATURE REVIEW

An extensive analysis of the existing literature on cyber security has been conducted in a paper by Bordoff in which the authors synthesized areas of various types of cyber threats and their impact on individuals and organizations. In another paper by Ahmed, the authors propose a method for applying security requirements to business processes through collaboration between business and security analysts [3]. In a research paper by Halder and Jaishankar, they emphasize the need to view cybercrime from a gender perspective, particularly cybercrimes against women. They highlight the various forms of cybercrimes faced by women, such as

revenge porn, online harassment, and cyberstalking. According to Halder and Jaishankar, cybercrimes against women are deliberate acts aimed at inflicting psychological and physical harm using modern telecommunication networks and cell phones [4]. According to the National Crime Records Bureau's data for the year 2020, the number of reported cybercrime cases in India has been on the rise with a significant increase in incidents targeting women [5].The Indian judicial system has various laws and policies in place to address cybercrimes, but there are several loopholes that hinder efforts to combat cybercrimes against [6]. These loopholes include a lack of awareness about cyber security measures among women, limited access to legal resources, and delays in the judicial process. This research investigates the cybercrime scenario in India against women.

III.   METHODOLOGY

This research used secondary data collected from different sources related to the cyber security of women in India. The sources include academic research papers, reports from government organizations and NGOs, and news articles. Based on the research papers and sources mentioned, it is evident that cybercrimes against women in India are a growing concern.

IV.   RESULTS & DISCUSSION

4.1 What is a Cyber Crime?

A cybercrime refers to any criminal activity that involves the use of computers, computer networks, or the Internet. Cybercrimes can take various forms, including hacking, identity theft, online fraud, cyberbullying, harassment, stalking, and dissemination of offensive content. Cyber Crime is a punishable act under the Information Technology Act, 2000 and there are legal consequences under the Indian Penal Code. Women are more vulnerable to cybercrimes due to societal restrictions and judgments, leading to fear of negative portrayal through online channels. These crimes are motivated by anger, lust, or personal vendettas, with little regard for the impact on victims and their loved ones [2].

4.2 Some of the Major Cyber Crimes Faced by Women in India

According to the research, some of the major cybercrimes faced by women in India include:

1 *Revenge porn:* This refers to the non-consensual sharing of intimate or sexual images online, which can cause extreme distress and harm to the victim [7]

2.*Cyber harassment and online stalking:* Women are often targeted with abusive, threatening, or harassing messages or behavior online, leading to psychological trauma and fear for their safety.

3. *Identity theft and online fraud:* Women are susceptible to having their personal information stolen and misused, resulting in financial loss and damage to their reputation.

4. *Online bullying and cyberbullying: Women* may be subjected to online bullying, including hate speech, body shaming, and intimidation, which can have severe psychological effects on their well-being and self-esteem.

5.*Cyber grooming:* Women, especially young girls, are targeted by individuals who establish online relationships with the intention of exploiting and manipulating them for sexual purposes.

6. Non-consensual dissemination of private and sensitive images: Women's intimate photos or videos may be shared without their consent, leading to humiliation, blackmail, and extortion.

7. *Online harassment and threats:* Women may face online harassment, including sexist remarks, threats of violence, and hate speech, which can create a hostile and unsafe online environment for them.

8.*Cloned Profiles:* One prevalent type of cybercrime involves the creation of fraudulent or cloned profiles, which conceals the true identity of the perpetrators and complicates efforts to identify them. Women get several messages from cloned profiles and at times they make fake profiles of an already existing person to befriend women and get information about them.

9. *Cyber Trolling:* Trolling means intentionally posting nasty, insulting, vulgar comments on someone's post either to demoralize them or to grab their attention. Trolling is a commonly used term among celebrities. Very often they see a lot of hatred in form of comments from fake profiles who do not admire their work.

10.*Cyber Morphing:* Morphing refers to the process of using computer graphics to alter the appearance of an image, making it appear original. Cyber Morphing involves the unauthorized use of women's images to create pornographic content, often by cropping and morphing their original photos into explicit images. Then the pictures are uploaded by the cloned profiles on different websites[2].

4.3 Some of the Existing Laws and Policies in India to Protect Women from Cybercrimes

In an effort to address the increasing cybercrimes against women in India, the government has implemented several laws and policies aimed at protecting women's rights and safeguarding them from cybercrimes.

   a.   *The Information Technology Act 2000:* This is the primary legislation that deals with cybercrimes in

India. It provides legal provisions related to cybercrimes and their punishments, including offenses like hacking, identity theft, and cyberbullying. The act also includes provisions for the protection of women's privacy and safety in cyberspace. Section 66C of the Information Technology Act deals with cases of cyber hacking, where personal information is fraudulently extracted and misused to cause mental and emotional harm to the victim, especially women. Section 66E of Information Technology Act provides protection against situations where any person is caught capturing, sharing, or posting on cyberspace the private part of a person without their consent shall be liable to imprisonment or fine or both. Section 67 and Section 67A of the Information Technology Act specifically address the publication or transmission of obscene or sexually explicit material online, including content that is harmful to women [2]. National Crime Records Bureau data for the year 2020 indicates that cybercrimes against women in India are on the rise [2]. The government has also introduced various amendments to the Information Technology Act, such as the IT Act 2008, to address new forms of cybercrimes and strengthen the legal framework for women's protection in cyberspace.

b. *Indecent Representation of Women (Prohibition) Bill, 2012:* This act punishes those who try to portray the indecent image of women in form of images or videos. This Bill has broadened its scope and now includes the online content as well. The bill includes Section 5 and Section 6 which specifically address the publication or transmission of obscene material depicting women [2].

Section 5: This section gives power to the officer to enter, and search any premises at a reasonable time in the region and can examine, and seize any obscene content whom they presume has convicted the offense.

Section 6: This section states the penalties which include imprisonment from 6 months to 5 years and a fine can be imposed from   10,000 to   50,000.

Additionally, the Criminal Law Act 2013 was enacted in response to the brutal rape and murder of a young woman in Delhi in 2012, which introduced stricter punishments for sexual offenses, including those committed online. Furthermore, the Indian government has launched initiatives such as the Women and Child Safety on Social Media Platform to address cybercrimes against women specifically.

The findings from various sources highlight the widespread issue of cybercrimes against women in India and their detrimental effects on their well-being and safety. Women in India face a multitude of cybercrimes, including online harassment, online stalking, cyberbullying, cyber grooming, non-consensual dissemination of private images, and online sexual exploitation. These cybercrimes are facilitated by factors such as gender-based discrimination, limited computer literacy among women, and a lack of awareness about cybercrimes. Furthermore, the findings also suggest that women in India are reluctant to seek legal justice for cybercrimes due to various reasons, including social stigma, fear of retaliation, and a lack of trust in the judicial system's ability to provide justice. The existing laws in India, such as the Information Technology Act of 2000 and the Indecent Representation of Women Bill, 2012, provide some legal provisions to address cybercrimes against women .

However, there are several loopholes and challenges in the implementation of these laws, which hinder efforts to effectively combat cybercrimes and ensure the safety and security of women in India. These challenges include the lack of a global consensus on the definition and classification of cybercrimes, inadequate legal powers for investigation and access to computer systems, jurisdictional challenges in cases of cross-border cybercrimes, and the need for capacity-building and awareness programs for law enforcement agencies, judiciary, and cybersecurity professionals [8].

Moreover, the findings also highlight the underreporting of cybercrimes against women in India. This underreporting can be attributed to various factors such as the lack of awareness about cybercrimes, fear of social stigma and retaliation, and distrust in the ability of law enforcement agencies to provide justice. The Apex Judicial body in the Country, Supreme court has also raised concern about the increasing cyber crimes especially against women [9].

Preventing cybercrimes against women demands a collective endeavor from individuals, institutions, and authorities [10]. Women should be given awareness on using devices securely, maintaining strong passwords, being cautious while sharing personal information online, and reporting any incidents of cybercrimes to the appropriate authorities. Additionally, educational institutions play a vital role in promoting digital literacy among women and girls.

V. CONCLUSION

In conclusion, the cyber security of women in India is a critical issue that needs immediate attention. While the Indian government has taken steps to address cybercrimes against women through legislation and initiatives, there are still several challenges that need to be addressed. These challenges include the need for more proactive measures to prevent cybercrimes, improved access to information and resources on cyber security for women, and enhanced implementation and enforcement of existing laws. Additionally, there is a need to bridge the gender gap in terms of digital literacy and technology access among women in India.

References

[1]*Most Crimes Against Women In 2022 Of Violation Of Right To Dignity ....* (n.d). https://www.ndtv.com/india-news/most-crimes-against-women-in-2022-of-violation-of-right-to-dignity-womens-panel-3654897

[2] Gupta, S., &Jaggarwal, S. *A Descriptive Study On Cyber Crimes Against Women With Reference To Cyber Security Law*.

[3] Dzhalladova, I., Škapa, S., Novotná, V., &Babynyuk, A. (2019, September 21). *Design and Analysis of a Model for Detection of Information Attacks in Computer Networks.* https://scite.ai/reports/10.24818/18423264/53.3.19.06

[4] Filinovych, V V. (2020, October 8). *Problems Of Human Rights Violations Caused By Cybercrimes And Ways To Overcome Them.* https://scite.ai/reports/10.18372/2307-9061.56.14904

[5] Balabantaray, S R., Mishra, M., &Pani, U. (2023, January 18). *A Sociological Study Of Cybercrimes Against Women In India: Deciphering The Causes And Evaluating The Impact On The Victims.* https://doi.org/10.21315/ijaps2023.19.1.2

[6] Secretariat, C. (2023, February 3). *Addressing Online Violence Against Women and Girls in the Commonwealth Asia Region.* https://scite.ai/reports/10.14217/comsec.1097

[7] Kumar. (2019, October). *Cyber Crime Against Women: Right To Privacy And Other Issues. Journal Of Legal Studies And Research*, *5*(5), 154–166.

[8] Ajayi, E F G. (2016, August 31*). Challenges to enforcement of cyber-crimes laws and policy.* https://scite.ai/reports/10.5897/jiis2015.0089

[9]*Cyber crimes against women leads to loss of self-worth: Justice Bhat of SC.* (n.d). https://lsm99galaxy.com/india-news/supreme-court-judge-unveils-book-critiquing-indian-courts-handling-of-rising-cybercrimes-against-women-and-inadequate-laws-101683449217583.html

[10] R. (2023, February 28). *Cyber Crime Against Women Summit '23 - Civil20*. Civil20. https://c20.amma.org/cyber-crime-against-women-summit-23/

[11] Balabantaray, S R., Mishra, M., &Pani, U. (2023, January 18*). A Sociological Study Of Cybercrimes Against Women In India: Deciphering The Causes And Evaluating The Impact On The Victims.* https://doi.org/10.21315/ijaps2023.19.1.2