ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

A STUDY ON AWARENESS AND EFFECTIVENESS OF CYBERSECURITY LAWS IN TACKLING DIGITAL CRIME AGAINST INDIAN WOMEN

Ms. Sona Mariam Jacob

Assistant Professor

KSD's Model College (Autonomous), Dombivli (E).

Abstract:

In India, digital crimes against women are becoming a major issue on a daily basis. With the increase of social media usage, women from almost every age group are falling victim to issues like online stalking, identity theft, cyberbullying, non-consensual deep fakes, and much more. The objective of this study evaluates the level of awareness among Indian women regarding current cybersecurity laws and examines the effectiveness of these laws in the present scenario. The study scrutinizes major and important legislation such as the Information Technology Act, 2000 and how amendments to it deal with issues such as women cybercrime. The study also incorporates primary data and secondary data methods to assess how aware women actually are with respect to their rights and the issues that come when trying to tackle such cybercrimes. This research is aimed at revealing that despite the existence of laws, many women are unaware of cyber laws. It also emphasizes the hardship women face in the reporting and resolving of such crimes. The research highlights there is a need to raise awareness among women, and to make the legal system stronger to fight digital crimes. It stresses the need to put strong efforts to protect women in the digital world.

Keywords: *Cybersecurity laws, digital crime, women, awareness, Information Technology Act, cyber harassment, India.*

Introduction:

The digital revolution in India has significantly transformed the way individuals interact, work, and access information. With over half a billion internet users and increasing smartphone penetration, the digital space has become an essential part of everyday life. However, alongside its numerous benefits, this transformation has also given rise to new forms of crime, disproportionately affecting women. Digital crimes against women in India include cyberstalking, online harassment, doxxing, non-consensual sharing of intimate images, identity theft, financial fraud, and deep fake exploitation. These offenses not only threaten personal security but also reinforce existing gender inequalities by discouraging women's participation in digital spaces.

Despite the presence of legal safeguards, such as the Information Technology (IT) Act, 2000, and relevant provisions under the Indian Penal Code (IPC), cybercrimes against women remain alarmingly prevalent. Many cases go unreported due to fear of social stigma, lack of awareness, and inadequate responsiveness from law enforcement agencies. Furthermore, the anonymity of perpetrators and jurisdictional challenges in cyber investigations make legal enforcement difficult. The psychological and social consequences of these crimes, including anxiety, depression, and reputational damage, further

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

highlight the urgent need for stronger protective mechanisms.

This research paper aims to analyze the growing menace of digital crimes against Indian women, explore legal and social challenges in addressing them, and propose strategies for ensuring safer digital spaces. By incorporating statistical insights, case studies, and an evaluation of existing laws and policies, this study seeks to contribute to the broader discourse on cyber safety and gender justice in India.

Types of Digital Crimes Against Indian Women:

Digital crimes against women in India manifest in several forms, including:

1. ***Cyberstalking*** – Continuous and unwanted online surveillance, threats, or intimidation through emails, social media, or other digital platforms *(Bansal & Arora, 2021).*
2. ***Online Harassment and Trolling*** – Abusive messages, character assassination, and targeted misogynistic comments, especially on social media *(Chakraborty, 2020).*
3. ***Doxxing*** – The public release of a woman's personal information, including addresses and phone numbers, with the intent to harass or harm *(Kumar & Agarwal, 2022).*
4. ***Non-Consensual Image Sharing (Revenge Porn)*** – The distribution of intimate images or videos without consent, often as an act of revenge or blackmail *(Gupta, 2019).*
5. ***Deepfake and Morphed Images*** – AI-generated or manipulated content portraying women in compromising situations to damage their reputation or extort money *(Sharma, 2021).*
6. ***Identity Theft and Financial Fraud*** – The unauthorized use of personal information for fraudulent activities, including credit card fraud and fake social media profiles *(Rao, 2020).*
7. ***Honey Trapping and Sextortion*** – Trapping victims into fake relationships or sexual exchanges and later using the content to extort money or favors *(Singh & Verma, 2018).*
8. ***Fake Job Offers and Online Scams*** – Scammers posing as recruiters to deceive women into sharing sensitive personal information or financial details *(Mishra, 2021).*

Review of Literature:

1. **Tarannum (2024)** elaborates on the different types of cyber crimes perpetrated against women, namely cyber-stalking, identity theft, and the non-consensual posting of explicit content. The study brings to light that, although there are laws in place, such as the Information Technology (IT) Act, 2000, difficulties in the enforcement of these laws and loopholes in the laws may never allow proper protection to women. The author proposes a multi-faceted solution, including increased training in digital literacy, bolstered legal protections, and cooperation between law enforcement and civil society.
2. **Halder & Jaishankar (2011)** study focuses on the revolution of women in the digital world, saying that the introduction of social media has helped women socially and economically. However, these new opportunities have, in many cases, rendered women more vulnerable to cyber harassment, online blackmail, and identity theft. The study shows how patriarchal ideologies continue to silence victims- thus implying better cybersecurity policies and law enforcement.
3. **Kushwaha & Prakash (2023)** take into consideration various industries, such as telecommunications and social media companies, which serve to detect that their users have been the victims of cybercrime against women. They further observe that more than half of the internet users are not able to recognize cybersecurity measures to be

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

taken; this renders them easy victims of exploitation online. The authors stressed the need for detection mechanisms based on AI and specialized training for investigators to deal with this growing phenomenon.

4. **Jaiswal (2022)** This study does a critical analysis of the effectiveness of cybercrime laws in India where he stated that traditional legal frameworks lag behind the fast-changing digital landscape. The research explains how cyber offenses, such as phishing, cyber defamation, online financial frauds, and many others, often escape the eye of law due to jurisdictional challenges and insufficient legal definitions.
5. **Mehta & Singh (2013)** study mentions that there is minimal awareness regarding cyber laws in Indian society, which also includes a lack of training for law enforcement bodies to effectively handle cases of cybercrime. The study recommends introducing digital literacy programs and cybersecurity education in school curricula to increase awareness.
6. **Kapoor (2023)** investigates the varying impact of cybercrimes on the genders and states that women face difficulty in reporting online offenses because of the stigma associated with it and weak legal protections. The research identifies various types of cyber violence including, but not limited to, cyberstalking, cyberbullying, and cyber extortion while the author recommends better victim recovery provisions and legal interventions for justice.
7. **Anand (2023)** the research has critically evaluated the cyber laws concerning the IT Act, 2000, and its provisions to deal with cybercrime. It pointed out the legislative gaps and the necessity of neighborhood cooperation in battling cross-border cybercrime.
8. **Dar & Nagrath (2022)** investigate whether women in India are the soft target for cybercrimes, stressing that deep-rooted gender biases, lack of awareness, and weak law enforcement have made women more vulnerable. The study calls for legal reforms, awareness campaigns, and enhanced penalties to stop cyber violence against women.

Rationale of the Study:

As digital technology grows in India, cybercrimes against women are rising sharply. Women experience online harassment, cyberstalking and privacy violations at higher rates than men, frequently suffering long-term psychological and social consequences. Many women are failing to report crimes due to lack of awareness of cyberlaw. This thorough study seeks to understand the level of awareness among women regarding cyber law and how efficacy of existing laws and preventative measures in combating digital crimes against Indian women.

Objectives of the Study :

1. To understand the concept of cyber violence against women
2. To assess the level of awareness among Indian women about cybersecurity laws.
3. To evaluate how effective these laws are in tackling digital crimes.
4. To identify challenges women face in reporting and resolving digital crimes.

Scope of the Study:

1. This research study looks at digital crimes against women in India and the cybersecurity laws.
2. It covers the awareness among women, the effectiveness of the law enforcement in cyber threats, and the legal structure.
3. The research was done using 100 respondents from different demographic groups in India.

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

Research Methodology:

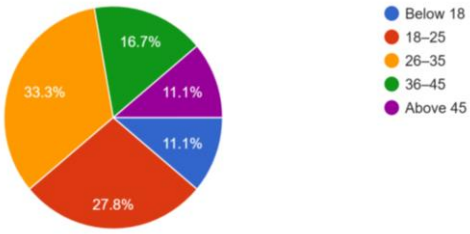
This study focuses on descriptive research design and convenience sampling in data collection. Google Forms questionnaire to get data on 100 respondents. This data included various demographic groups in terms of awareness and perception of cybersecurity laws. The respondents were drawn from many areas in India to achieve diversity. Moreover, secondary data was collected from magazines, thesis reports, seminars and conference papers, articles, websites, unpublished data, published books, journals, and newspapers etc

Limitations :

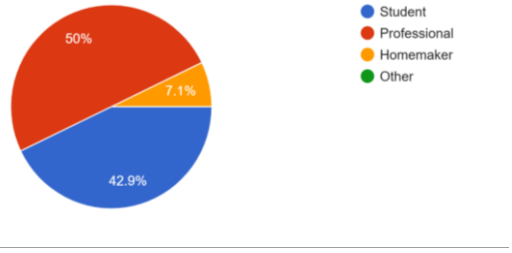
1. Sample size is small because of the time constraint.
2. The present study is restricted to analyse basic awareness of cyber law among women in india.
3. The perception of respondents towards cyberlaw may differ according to their personal experiences.
4. The study is based on convenient sampling, meaning the sample may not be fully representative of the entire population.

Data Analysis:

Age

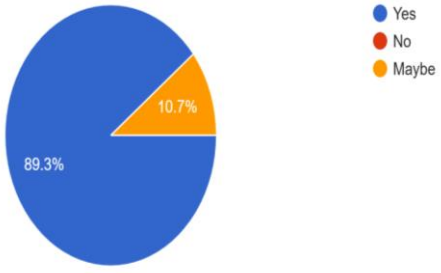


Occupation

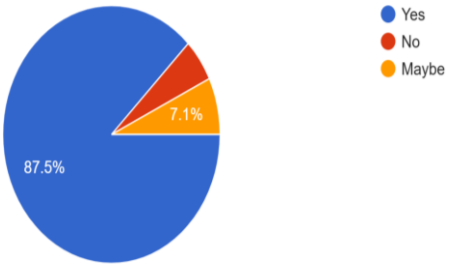


- **Age Distribution**: All the 100 respondents were females, in the age group of below 18 (11.1%), 18-25 years (27.8%), 26-35 years (33.3%), 36-45 years (16.7%), and above (11.1%).
- **Occupation**: Of the total respondents, 50 percent were professionals, while students accounted for 42.9 percent of the respondents. And the remaining respondents were only about 7.1 percent who were housemakers.

Are you aware of cybersecurity laws in India?



Have you heard about the IT Act, 2000, and its provisions related to online safety?



ISSN–2277- 8721

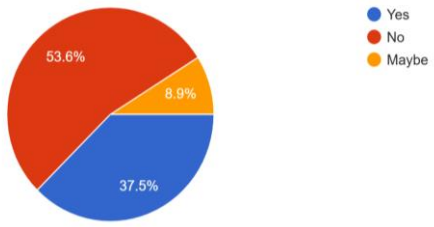
EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

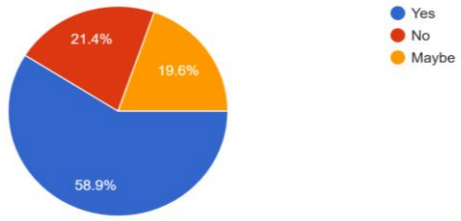
OPEN ACCESS Original Research Article

- **General Awareness of Laws in India**:
  A significant majority (89.3%) of respondents were aware of laws in India, while 10.7% were not. This suggests a relatively high level of legal awareness among the surveyed population.
- **Awareness of the IT Act, 2000**:
  87.5% of respondents had heard about the IT Act, 2000, and its provisions related to online safety. However, 5.4% didn't know about it, and 7.1% weren't sure. This means a small but important group of people don't know much about this key law.

Do you know that Section 354D (cyberstalking) and Section 66E (privacy violation) specifically address crimes against women?

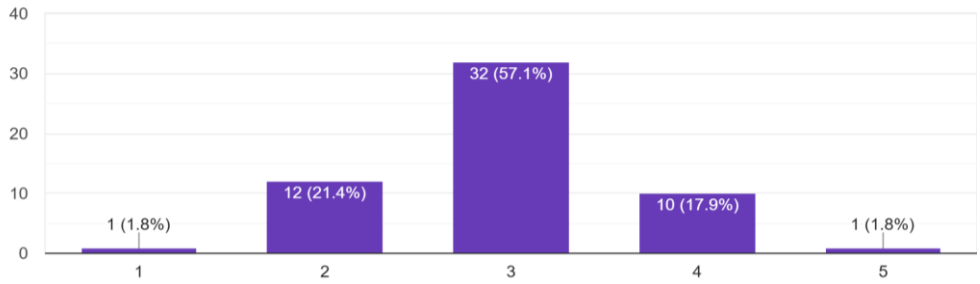


Do you believe that public awareness campaigns are sufficient to educate women about digital safety and laws?



- **Awareness of Specific Provisions (Section 354D and 66E)**:
  53.6% of respondents were unaware of Section 354D (cyberstalking) and Section 66E (privacy violation), both of which specifically address crimes against women. But again 37.5% expressed awareness, while 8.9% put themselves in a state of uncertainty, indicating a gap in knowledge regarding the provisions for these specific legal protections.
- **Public awareness campaigns are sufficient to educate women about digital safety and laws:**
  A majority (58.9%) of respondents have mentioned that public awareness campaigns have been sufficient for educating women regarding digital safety and laws. While only 21.4% of respondents expressed futility over public awareness campaigns, and 19.6 % put themselves in a state of uncertainty which emphasized the necessity of stronger and wider awareness campaigns.

How would you rate your knowledge of cybersecurity laws in India?
Rate on a scale of 1–5: 1 = No Knowledge, 2 - Basic knowledge 3 = Moderate knowledge, 4 = Solid knowledge, 5 = Excellent Knowledge.



ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

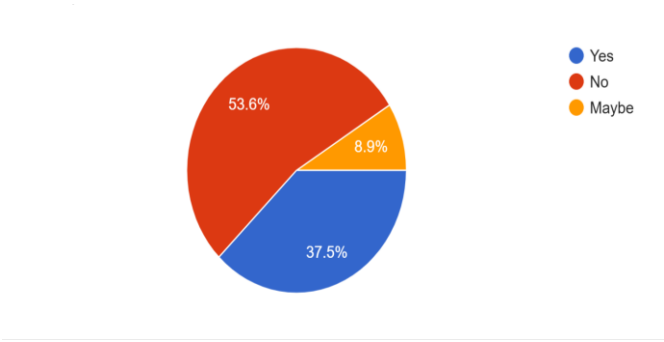
Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

- **Knowledge of cybersecurity laws in India**

  Most respondents (57.1%) rated their knowledge of cybersecurity laws as moderate, while 21.4% had basic knowledge, and 17.9% had solid knowledge. Only 1.8% rated their knowledge as excellent, while another 1.8% had non-existent knowledge. This shows that while the majority had some understanding of cybersecurity laws, there is still a widening gap.

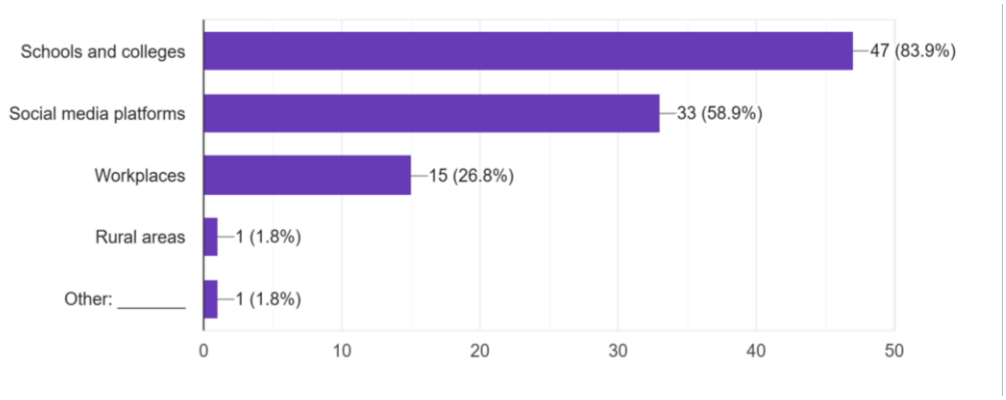
Are you aware of any helplines or online platforms where digital crimes against women can be reported?



- **Awareness of Helplines or Online Platforms**:

  53.6% of respondents were unaware of helplines or online platforms for reporting digital crimes against women, while 37.5% were aware about it, and 8.9% were uncertain. This suggests that a significant portion of the population may not know where to seek help in case of digital crimes

Where do you think awareness about cybersecurity laws should be spread more actively?



- **Areas for Spreading Awareness**:

  Schools and colleges (83.9%) and social media platforms (58.9%) were identified as the most important areas for spreading awareness about cybersecurity laws. Workplaces (26.8%) and rural areas (1.8%) were seen as less

ISSN–2277- 8721

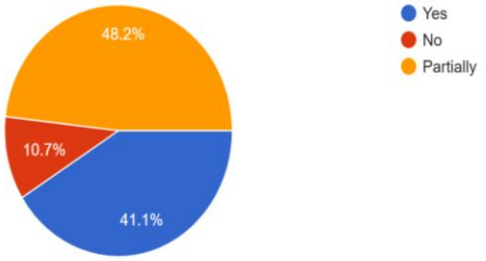
EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

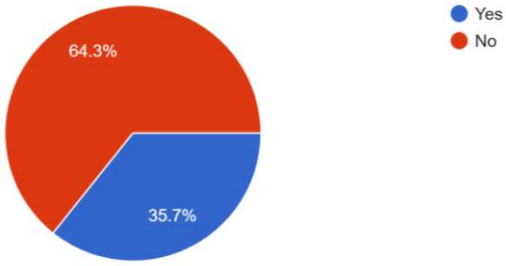
OPEN ACCESS Original Research Article

critical, possibly due to the demographic profile of the respondents.

Do you feel Indian cybersecurity laws are adequate in protecting women from digital crimes?

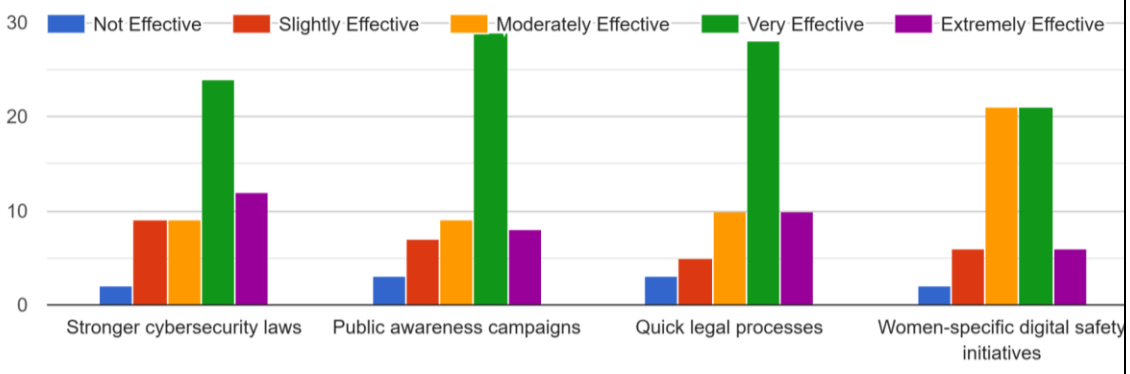


Have you or anyone you know reported a digital crime?



- **Adequacy of Laws in Protecting Women**:
  48.2% of respondents believed that Indian cybersecurity laws are only partially adequate in protecting women from digital crimes, while 41.1% felt they are adequate.Only 10.7% believed that the laws were inadequate for the same purpose. This finding, however, gives a positive outlook toward the legislative arrangements, to say the least, but there is still an opportunity to improve.
- **Experience with Reporting Digital Crimes**:
  A vast majority (64.3%) of respondents had not reported a digital crime, while only 35.7% had. This low reporting rate could be due to a lack of awareness, fear of stigma, or dissatisfaction with the legal process.

How effective do you believe the following measures will be helpful in combating digital crimes?



ISSN–2277- 8721

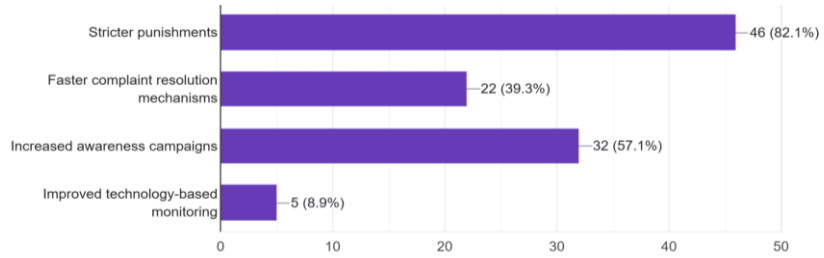
EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

- **Measures to Combat Digital Crimes**:
  Respondents rated stronger cybersecurity laws , public awareness campaigns, quick legal processes, and women-specific digital safety initiatives as moderately to very effective in combating digital crimes. This suggests that a multi-pronged approach is needed to address the issue effectively.

What measures would you recommend to improve cybersecurity laws for better protection of women?



- **Perceived Effectiveness of Measures to improve cybersecurity laws**:
  Respondents believed that stronger cybersecurity laws (82.1%), faster complaint resolution mechanisms (39.3%), and increased awareness campaigns (57.1%) would be effective in combating digital crimes. Stricter punishments and improved technology-based monitoring (8.9%) were also recommended, though to a lesser extent.

1. **NCRB Data on Cyber Crimes Against Women:** According to the reported NCRB 2021, there is a significant increase in cyber crimes, especially that related to women, in India. Out of the 50,035 cybercrimes reported by NCRB in 2021, 32% (16,013) pertained to crimes against women. The upsurging statistic reflects an alarming web of crime on the rise, with significant spikes in cases such as cyberstalking, online harassment, and identity theft.
   NCRB report indicate the following:

I) 30% of the reported cyber crimes against women are cases of cyberstalks and online harassment. Social media platforms often provide the needed connection for the same, permitting the perpetrator to remain camouflaged.

II) Identity theft and morphing (manipulation of images and videos) recorded a 22% increase over the last year.

III) What the report did reveal was the rising number of women, which has amounted to an increase of about 25% in the reporting of yearly cybercrimes from 2021-2020. More importantly, recognition has gained momentum as has the number of women reporting it. Yet, while this recognition has encouraged more reports, the conviction rate throughout stood at a meager 12%.

2. **Government Initiatives and Awareness**
   The government of India has started various initiatives to counter women-centered

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

cybercrimes, which include:

I) Cyber Crime Awareness and Prevention for Women and Children: It was initiated by the Ministry of Home Affairs to help women, girls, and children learn about cybercrimes and provide resources enabling them to avoid being the victim of these heinous crimes.

II) National Cyber Crime Reporting Portal: Set up in January 2019, this platform allows speedy reporting by the victims of cybercrimes. Over 100k cases have been reported on this portal for the period of 2021–2022, where 45% of the victims were women.

However, according to a survey conducted by the Federation of Indian Chambers of Commerce & Industry (FICCI), there has been an increase in awareness of such portals and initiatives, but significant gaps still remain in rural areas, as follows:

- 60% of urban women were aware of the National Cyber Crime Reporting Portal.
- 38% of women in rural areas reported having knowledge of the portal and how it can be used to report cybercrimes.
- Whereas 45% of urban women were aware of the Cyber Crime Awareness Programs, only 30% of rural women had heard of these programs.

3. Breakthrough India and Cyber Peace Foundation data on Women's Awareness of Cybersecurity Laws:

The organizations that have provided some more information about this awareness around cyber laws include Breakthrough India and Cyber Peace Foundation:

I) According to the Breakthrough India report, 70% of women had faced online harassment in a 2022 study. Though almost half were able to communicate the experience to law enforcement, only 45% of these women knew the laws they could resort to when faced with discrimination.

II) Though 80% of the women surveyed by the Cyber Peace Foundation knew the concept of cybercrime, only about 50% were aware of any laws protecting them against online harassment or abuse, such as Information Technology (IT) Act or Section 499 against defamation and Section 506 of the Indian Penal Code (IPC).

Conclusion: This study finds that there exists a social disparity and gap in both enforcement and awareness of laws governing cyberspace with all the provisions meant to protect women in India. Study reports highlight a growing trend concerning cyber offenses against women, including cyberstalking, identity theft, and online harassment.The conviction rate is still extremely low, which is a reflection of ineffective legal and law enforcement procedures. Barriers such as limited internet access, digital illiteracy, and a lack of awareness about legal protections disproportionately affect women, particularly in rural areas. Most individuals are only aware of basic cybersecurity laws, with little to no understanding of specific legal provisions. This lack of legal literacy further weakens their ability to seek justice or take preventive measures. The general hesitancy to report cybercrimes is a worrying trend that is fueled by shame, mistrust of the legal system, and drawn-out court cases. Many respondents also voiced doubts over the efficacy of current programs in educating women about cybersecurity, as they are treated as fully ineffective or occasionally moderately effective. These results highlight the fact that although laws are in place to safeguard women online, it is still very

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

difficult to guarantee that they are widely known, easily accessible, and upheld. Stronger legal enforcement, better digital education, and programs that increase public confidence in the legal system are necessary to close these gaps, promote reporting, and provide protection thereafter.

Suggestions:

1. Strengthening the IT Act, 2000, through harsh punishment for the repeat offenders; faster legal proceedings through cybercrime courts.
2. Training law enforcement agencies in handling gender-sensitive cases of cybercrime and setting up dedicated district-level cybercrime cells.
3. Raising awareness, especially in rural areas, through digital literacy programs in schools, colleges, and community centers, supplemented by regional-language outreach campaigns.
4. Facilitate such reporting of incidents of cybercrime/harassment through the formulation of easily accessible reporting mechanisms, which include the setting up of a 24/7 cyber crime helpline, mobile applications available for anonymous reports, and setting up of offline legal aid clinics to enable women to report crimes without any fear.
5. Develop campaigns that challenge the stigma of reporting and encourage women to bring forth such criminal acts without any hesitation.

References:

1. *Press Information Bureau, Government of India. (2023, February 1). Information Technology Act, 2000 and the Indian Penal Code (IPC) https://pib.gov.in/PressReleasePage.aspx?PRID =1881404*
2. *National Commission for Women. (n.d.). Cyber crime prevention against women and children (CCPWC) scheme. https://ncw.nic.in/ncw-cells/legal-cell/new-bills-laws-proposed/cyber-crime-prevention-against-women-and-children-ccpwc*
3. *Bansal, R., & Arora, P. (2021). Cyberstalking in India: An emerging threat to women's safety. International Journal of Cyber Law, 8(2), 45-60.*
4. *Chakraborty, A., Saha, R., & Bose, P. (2020). Trolling and harassment on social media: A gendered perspective. Journal of Digital Ethics, 12(3), 112-130.*
5. *Gupta, S. (2019). Revenge porn and privacy rights: Legal challenges in India. Cyber Law Review, 10(4), 78-95.*
6. *Kumar, D., & Agarwal, V. (2022). Doxxing and cyber victimization of women: A critical review. Indian Journal of Law and Technology, 14(1), 32-55.*
7. *Mishra, N. (2021). Online job scams and financial fraud: A growing threat for women in India. Economic & Cybersecurity Journal, 9(2), 88-102.*
8. *Rao, K. (2020). Cyber fraud and identity theft: The vulnerabilities of Indian women. Journal of Information Security, 7(1), 50-67.*
9. *Sharma, P. (2021). Deepfake technology and the dangers of AI-based exploitation of women. Technology and Law Review, 11(3), 120-140.*
10. *Singh, R., & Verma, A. (2018). Sextortion and honey trapping in digital India: Emerging trends and legal challenges. Indian Cyber Law Journal, 6(2), 67-85.*
11. *Tarannum, M. (2024). Cyber Crimes against Women in India: An Analysis. Central University of Kashmir Law Review, 4, 133-147.*
12. *Halder, D., & Jaishankar, K. (2011). Cyber Crime and the Victimization of Women: Laws, Rights, and Regulations. IGI Global.*
13. *Kushwaha, N. S., & Prakash, P. (2023). Legal Framework and AI Strategies in Addressing Cybercrime Against Women in India: Role of*

ISSN–2277- 8721

EIIRJ Electronic International Interdisciplinary Research Journal

Volume–XIV, Special Issues – I Jan – Feb 2025

OPEN ACCESS Original Research Article

Intermediaries in Detection of Cybercrime. Journal of Cyber Security and Digital Forensics.

14. *Jaiswal, K. (2022). Effectiveness of Cybercrime Laws and Regulations in India: A Critical Study. BBDU Law Journal.*
15. *Mehta, S., & Singh, V. (2013). A Study of Awareness About Cyber Laws in the Indian Society. International Journal of Computing and Business Research, 4(1), 1-8.*
16. *Kapoor, T. (2023). Cyber Crime Against Women in India: Identification and Mitigation. Indian Journal of Integrated Research and Law, 3(1), 1-15.*
17. *Anand, M. (2023). Cybercrime and Cyber Laws in India. Indian Journal of Law & Legal Research, 5(2).*
18. *Dar, S. A., & Nagrath, D. (2022). Are Women a Soft Target for Cyber Crime in India? Journal of Information Technology and Computing, 3(1), 23-31.*
19. *National Crime Records Bureau. (2021). Crime in India Report. https://ncrb.gov.in/*
20. *Ministry of Women and Child Development. (2021). Annual Report on Women's Safety. https://wcd.nic.in/*
21. *Breakthrough India. (2022). Digital Safety Survey for Women.https://www.breakthroughindia.org/*
22. *The Cyber Peace Foundation. (2021). Digital Safety Awareness Report. https://www.cyberpeace.org/*
23. *Federation of Indian Chambers of Commerce & Industry (FICCI). (2022). Survey on Cybercrime Awareness and Reporting Among Women. https://www.ficci.in/*

Cite This Article:

***Ms. Jacob S.M.* (2025).** *A Study on Awareness and Effectiveness of Cybersecurity Laws in Tackling Digital Crime Against Indian Women.* **In Electronic International Interdisciplinary Research Journal: Vol. XIV** (Number I, pp. 132–142).