ASSESSING THE EFFECTIVENESS OF CYBER LAW IN TACKLING CYBER CRIME AGAINST WOMEN IN INDIA: A CASE STUDY OF DELHI

Vikas Ireshrao Kunthewad

ABSTRACT

In the digital age, cybercrime against women has become a significant issue that compromises security, privacy, and dignity. The objective of the research was to analyze the effectiveness of cyber laws in controlling cyber-crimes against women in Delhi. The study uses a qualitative research methodology. Simple random sampling was used to choose 440 responders in total. Structured questionnaires were used to gather data, which was then analysed to test the premise that cybercrime against women may be effectively prevented by enforcing cyber laws. According to the objective of the study, both null hypothesis and alternative hypothesis were developed. To test the hypotheses, the Chi-square test was used. It was concluded that enforcement of cyber laws is effective in checking cybercrime against women. The study recommends building specialized cybercrime teams, strengthening law enforcement and ensuring quicker legal processes through fast-track courts.

Keywords: Cybercrime, Cyber law, enforcement, Digital safety, Women's protection etc.

1. INTRODUCTION

Globally, the quick development of digital technology has changed how people communicate, do business, and share information. Unprecedented prospects for socioeconomic development and interpersonal interaction have been brought about in India by the widespread use of cellphones, social media, and internet access. But along with these developments, the digital realm has also given rise to new types of criminal activity, which are commonly referred to as cybercrime. Cybercrime includes any unlawful activity conducted via computers, networks, and the internet, from identity theft and hacking to online abuse and exploitation. Because of gender prejudices and the anonymity that cybercriminals have, women in particular have become more vulnerable to such crimes.

There are many different types of cybercrime against women, such as identity theft, online defamation, revenge pornography, cyber stalking, cyber bullying, email spoofing, and threats of violence. These behaviours frequently result in serious emotional suffering, harm to one's reputation, and, in the worst situations, bodily injury. The impact of such crimes is heightened in a nation like India, where patriarchal traditions and gender inequalities are still pervasive.

Victims are often deterred from reporting occurrences because they fear social shame or lack confidence in the legal system. The Information Technology Act of 2000 & other provisions of the Indian Penal Code (IPC) provide the main legal base for combating cybercrime in India. Amendments have been made throughout time to meet new concerns in the digital sphere, with clauses that target offences against women in particular.

Notwithstanding these legislative actions, questions remain about the efficiency of the legal system, victim care programs, and the efficacy of law enforcement, and the overall deterrence value of existing laws.

1.1 Relevance of the Study

Being India's capital, Delhi serves as a crucial example for assessing how well cyber laws work to prevent crimes against women. Delhi has seen a lot of people use the internet, e-commerce has grown quickly, and social media is quite popular, but it also has a high rate of online and offline crimes against women. Public discussion and policy attention have

been drawn to high profile instances of internet abuse and harassment in the city. As a result, evaluating Delhi's cyber law enforcement and execution can provide insightful information that can be applied to other Indian cities.

There are several reasons why this study is both essential and urgent. It first addresses the increasing need to assess whether the existing legal safeguards are sufficient to protect women online. Second, it highlights the real-world difficulties that victims, courts, and law enforcement organisations have when putting these laws into practice. Third, it makes policy suggestions meant to bridge the gap between the intentions of legislation and the realities on the ground.

1.2 Statement of the Problem

Cybercrime against women is on the rise in India, especially in major cities like Delhi, despite the existence of specialized cyber laws and punitive measures intended to protect women. Due to cultural pressures, administrative delays, lack of knowledge, and insufficient technical skills, many victims find it difficult to report events.

Training, resources, and jurisdictional difficulties are some of the limitations that law enforcement agencies frequently encounter. These elements cast doubt on the legislation' overall efficacy and undercut their potential deterrent effect. Therefore, there is an urgent need to investigate measures to improve the enforcement of present cyber laws and to rigorously assess their effectiveness in preventing such crimes.

1.3 Scope of the Study

The city of Delhi serves as a prominent example of urban India in this research. The scope is restricted to cybercrimes that specifically target women, including non-consensual picture sharing, cyber stalking, online harassment, and other forms of gender-based violence made possible by technology. Although national laws are part of the legal framework under consideration, Delhi's local enforcement methods, difficulties, and results are the main focus. It is anticipated that the results would be applicable to other Indian urban areas with comparable sociocultural and technical settings.

1.4 Significance of the Study

This research is important for many parties involved. It offers legislators an evidence-based

assessment of current legislation, pointing out any shortcomings that call for procedural or legislative changes. It highlights operational difficulties for law enforcement organisations and makes suggestions for resource allocation and capacity improvement. It helps civil society organisations create advocacy campaigns and awareness initiatives by illuminating victim experiences. Lastly, it adds to the body of knowledge on women, law, and technology, especially in the Indian context, for the academic community.

2. REVIEW OF LITERATURE

Ahlawat (2024) the study looks at the many kinds of cybercrimes that are perpetrated against women in India, examining the socio-legal consequences of these crimes as well as the legal and legislative responses to them. It draws attention to the serious effects that these crimes have on freedom of expression, mental health, and overall involvement of women in the digital economy. The study reveals flaws in current legislation using statistical analysis and case studies. The study ends by highlighting the growing issue of cybercrimes against women in India, outlining the extensive harm they do, and promoting better legal frameworks and remedies to address this problem.

Dar (2022) It has been determined that cyber violence against women is a serious problem with possible social and financial repercussions. Its widespread use is facilitated by social media, dissemination of information through mobile technologies. Any sexual violence against women that is made possible by information and communication technologies (ICTs), such as video games, mobile devices, and the internet, is called cyber violence. The misuse of these technologies has become a common means of inflicting abuse on women. Cybercrimes that specifically target women are discussed in the article, including phishing, digital stalking, online sex trafficking, cyber extortion, online bullying, and cybersex abuse (such as sending sexually explicit or pornographic emails). It highlights how deeply distressing a cybercrime can be for a woman, especially in India, where women are frequently undervalued and cybercrimes go unpunished by the judicial system. The study's conclusion discusses potential remedies for India's rising rate of cybercrimes against women.

It also talks about what victims may do and how the legal system has to be changed to address this expanding issue. The study emphasises the serious effects that cybercrimes have on Indian women, the different ways that these crimes manifest, the judicial system's

shortcomings, and the pressing need for victim assistance and legislative changes in order to successfully address this social issue.

Gribetz (2022) the function of the Indian legal system and the support that technology may provide in combating cybercrimes against women are particularly examined in this study. It also looks at how these components might give victims of these kinds of crimes the crucial help they need. Stalking, harassment, bullying, blackmailing, defamation, pornography, obscenity, morphing, e-mail spoofing, revenge porn, slut-shaming, and sexting are just a few of the offences that fall under the umbrella of cybercrimes against women. Unlike traditional crimes, these crimes enable offenders to act remotely. With technology playing a critical role in both prevention and victim assistance, the study concludes that although India has a legal framework to combat cybercrimes, the legal system needs to be significantly improved in order to handle these offences and provide women victims with adequate support.

Dubey (2021) in the report, many kinds of cybercrimes against Indian women are identified. These consist of, among other things, sexual harassment and abuse, email deception, and online defamation. Women who fall prey to cybercrime suffer from severe psychological effects that have a profound effect on their life. In extreme situations, these effects may potentially result in suicide. A study of the legal protections that Indian women have against cybercrime is presented in this research. One important conclusion is that women encounter obstacles when trying to take criminals to court. It is concerning that these difficulties exacerbate the anguish caused by the cybercrime. The report emphasises how common and varied cybercrimes are that target women in India, as well as the serious psychological harm they cause, and the substantial hurdles women encounter when seeking legal recourse.

Halder (2015) the study came to the conclusion that restorative justice (RJ) and therapeutic jurisprudential (TJ) techniques should be used to address cyber stalking as it is an emotional crime. The shortcomings of the present Indian legal system, particularly Section 354D of the Indian Penal Code, make it difficult to effectively address the needs of victims and promote genuine healing. For better victim assistance and justice in cyber stalking instances, the combination of RJ and TJ concepts is essential. The victim's true objectives, which may not always be severe punishment for the culprit but rather trauma recovery

through a restorative process, are frequently overlooked by the law. Current informal mediations sometimes conclude with only requesting that harassers cease their behaviour, with no appropriate procedural steps taken or victims' recompense provided. According to the research, India's cyber stalking laws should adopt a more comprehensive, victim-centered strategy that incorporates restorative justice and therapeutic jurisprudence concepts rather than merely retributive justice. This would promote a more efficient and compassionate judicial system by guaranteeing that victim' requirements for recovery, privacy, and redress are sufficiently satisfied.

3. OBJECTIVES OF THE STUDY

i. To analyze the effectiveness of cyber laws in tackling cyber-crimes against women in Delhi.

ii. To evaluate the challenges in implementing cyber laws for the protection of women in Delhi.

iii. To propose strategic recommendations for strengthening cyber law enforcement against crimes targeting women in Delhi.

4. MATERIALS & METHODS

4.1 Research Methodology

A systematic approach to problem-solving is known as a research technique. This field of study focuses on organizing and evaluating research methods. The systematic strategy and techniques used to collect, examine, and evaluate data for a research project is referred to as research methodology. It describes how the research was carried out, including the instruments, processes, and tactics used to achieve the study's goals. The study employed a qualitative approach to research.

4.2 Research design

Research design is a kind of strategy which directs researcher in logically and clearly arranging the many components of a study. It acts as the cornerstone for the methodology of the research. A research design acts as a structure or plan that directs the whole

investigation. With the help of a defined road plan, the researcher may conduct the research process in a methodical and systematic manner. It directs the investigation, guaranteeing that every stage is methodically and well prepared. In the research study, a descriptive research design was employed. The design is founded on theory and was created by gathering, analysing, and presenting facts.

4.3 Sample

The sample size of a research study is the total number of participants. It has a big impact on how reliable and useful the study's findings are, thus it's a crucial part of research design. A well-considered sample size ensures results that are trustworthy and transferable to a broader population. Because they offer higher statistical power, which increases the likelihood that the results will properly represent the actual population, bigger sample sizes are often preferred. Researchers may draw reliable conclusions and generalizations from the data when the sample is well-defined since it guarantees that the sample fairly reflects the larger population. Sample size was 440.

4.4 Sampling method

A sampling technique is a methodical approach to sample selection. This method makes the study more practical and economical by ensuring that researchers may collect data effectively without polling the entire community. One of the most popular sampling techniques is simple random sampling due to its fairness and impartiality. They used basic random sampling in their investigation. When every individual in the universe has an equal chance of selection, it ensures a fair and impartial representation. This approach eliminates selection bias, enhancing the accuracy, credibility, and broader applicability of research outcomes across the entire target group. There are several processes involved in putting simple random selection into practice. The target demographic must first be precisely identified. The next step is to establish a sample frame, which is a comprehensive list of every person in the population. Using instruments like lottery techniques, random number tables, or computerized random generators, researchers choose individuals at random from this list. By using these methods, selection bias is lessened and representative data may be gathered.

4.5 Data Collection

The study gathered primary data by using a well-designed structured questionnaire designed to assess awareness, experiences, and perceptions regarding the effectiveness of cyber laws in tackling crimes against women in Delhi. To get quantifiable answers, the survey had both closed-ended & Likert-scale items. Simple random selection was used to choose a sample size of 440 female respondents, ensuring inclusive representation across age groups, educational attainment, and professional backgrounds. To reach a larger population, the survey was administered both offline and online. Secondary data was gathered from government papers, court records, and pertinent scholarly works.

4.6 Data Analysis

The effectiveness of internet laws in addressing crimes against women in Delhi was investigated by methodically coding and statistically analysing the data that was gathered. To summarize the demographic characteristics, awareness levels, and opinions of respondents about the efficacy of law enforcement, descriptive statistics like frequencies and percentages were used.

To test the research hypotheses, the Chi-square test was applied. To ascertain if there is a significant correlation between categorical variables including knowledge of cyber laws, experiences of cybercrime, and opinions on the efficacy of enforcement, this non-parametric statistical test was selected. Since the majority of the data in this study comprised qualitative variables that were measured on nominal and ordinal scales, the chi-square test was especially suitable. The test offered an efficient way to compare observed and predicted frequencies without supposing a normal distribution, which was important given the goal of evaluating the link between respondents' experiences and their opinions on the efficacy of cyber laws.

Determining whether the implementation of cyber laws has a substantial influence on the control of cybercrime against women in Delhi was made easier by the Chi- square analysis results. The results of this study, which were backed up by primary and secondary data, served as the foundation for evaluating the efficacy of the laws in place and pinpointing areas in need of development.

5. RESULT & DISCUSSION

According to the study, three interconnected factors legislative sufficiency, enforcement capability, and public awareness determine how successful cyber laws are. The comprehensiveness and lucidity of legal laws pertaining to cybercrimes against women are referred to as legislative adequacy. The institutional, human, and technical resources that law enforcement organisations have at their disposal to identify, look into, and bring charges against criminals are referred to as enforcement capacity.

Public awareness pertains to women's understanding and readiness to use legal safeguards. The total effect of the law may be diminished by any shortcomings in these areas. Cybercrime is the biggest threat to society as a result of the Internet's transcendental jurisdiction. Women and children are the primary victims of this sin.

According to studies, there are 52 million internet users in India, and that number rose to 71 million in 2009. In 2009, 8% of working women and 7% of nonworking women were internet users, while 37% of all users accessed the internet through Cyber Café. It is a frequent occurrence for cyber café operators to easily divulge the key information of internet users, which is then utilised for unlawful purposes. While familiarity with technology is a positive aspect that is essential to any nation's development, it is also serving as the basis for an increase in technological offences against the weaker segments of society.

Additionally, statistics reveal that Delhi residents have very low levels of cyber knowledge. The IT Act's preamble makes it clear that improving e-commerce was its main objective; as such, it covers economic or commercial crimes including fraud, hacking, and confidentiality violations. But safeguarding internet users was unfamiliar to the drafters.

In India, women and children receive additional safeguards through the Constitution, Criminal Procedure Code, and IPC. For instance, Section 509 safeguards women’s modesty, while the IPC criminalizes acts such as rape, marriage (forced), kidnapping, & performing abortion without a woman’s consent. Until recently, there were no specific rules protecting women from cyber-crimes, despite the fact that the Indian constitution gives women the same rights as men in terms of their life, education, health, food, and job. Since the Delhi Gang Rape case (Nirbhaya Case) in 2012, there has been a lot of push to

enact tougher laws and harsher penalties to protect women from offenders.

The most recent law that deals with cybercrime against women is the Bharatiya Nyaya Sanhita, 2023. Under BNS, **Section 75** covers sexual harassment via electronic means (formerly IPC Sec. 354A). **Section 77** criminalizes unauthorized recording or sharing of intimate images similar to revenge porn (formerly IPC Sec. 354C). **Section 78** addresses cyber stalking (formerly IPC Sec. 354D). **Section 79** deals with outraging the modesty of a woman, which can extend to harassing online behaviors like deep fakes.

It is now feasible to appropriately deal MMS scandals, pornography, morphing, and defamation. Because the victim is reluctant, shy, and worried about her families image being damaged, most cybercrimes go undetected. She frequently feels that the crime that was perpetrated against her is her fault. Women are particularly at risk from cybercrime since the perpetrator's identity is anonymous and he may use a variety of names and identities to continuously threaten and blackmail the victim. Women worry that if they report the crime, it would negatively impact their family life. They also worry about whether they will receive support from their friends and family and how society will perceive them after learning about the crime. Women frequently neglect to report crimes because of these worries, which raises the spirits of the criminals.

5.1 Testing of Hypothesis

The following hypothesis was developed in accordance with the study's goals:

H_0 (Null Hypothesis): Enforcement of cyber laws is not effective in checking cybercrime against women.

H_1 (Alternative Hypothesis): Enforcement of cyber laws is effective in checking cybercrime against women.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Cyber-Crime Against women * Enforcement of Cyber Laws	440	100.0 %	0	0.0 %	440	100.0 %

Source: SPSS Output

The Case Summary provides essential information about the data preparation and completeness of the dataset before conducting a Chi-Square test. A Chi-Square test is being considered with the statistics as under:

Valid N: The number of cases (data points) with complete and valid information is 440. This constitutes 100% of the total dataset, indicating that there are no missing or incomplete values among the cases being analyzed.

Missing N: The number of cases with missing values is 0, accounting for 0% of the dataset. This signifies that there is no missing data to be concerned about in this analysis.

Total N: This refers to the total number of cases in the dataset, which is also 440. This aligns with the Valid N since there are no missing cases.

The Case Processing Summary illustrates the high data quality in this context, as the dataset is complete and lacks missing values. This is crucial for the reliability of statistical analyses like the Chi-Square test, as missing data can potentially skew results and lead to inaccurate conclusions. With a complete dataset of 440 cases, the Chi-Square test can be confidently conducted, producing meaningful insights or relationships between categorical variables under examination.

Cyber-Crime Against women * Enforcement of Cyber Laws Crosstabulation

			Enforcement of Cyber Laws		Total
			Effective	Ineffective	
Cyber-Crime Against women	Yes	Count	93	98	191
		Expected Count	111.1	79.9	191.0
	No	Count	163	86	249
		Expected Count	144.9	104.1	249.0
Total		Count	256	184	440
		Expected Count	256.0	184.0	440.0

Source: SPSS Output

Chi-Square Tests

	Value	df	Asymp. Sig. (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	12.495[a]	1	.000		
Continuity Correction[b]	11.815	1	.001		
Likelihood Ratio	12.502	1	.000		
Fisher's Exact Test					
Linear-by-Linear Association	12.466	1	.000	.000	.000
N of Valid Cases	440				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 79.87.

b. Computed only for a 2x2 table

Findings of the test

A chi-square test was conducted to test the hypothesis. The calculated chi-square value of 12.495 is more than the table value of 3.841. Therefore, researcher has enough evidence to reject the null hypothesis that enforcement of cyber laws is not effective in checking cybercrime against women.

6. CONCLUSION

This study looked at the effectiveness of Delhi's internet laws in combating crimes against women, the difficulties in putting them into practice, and potential ways to make them better. Analysing how well cyber laws in Delhi address cybercrimes against women was the first goal. The computed Chi-square value of 12.495 was greater than the table value of 3.841, according to examination of data gathered from 440 respondents using simple random sampling and the Chi-square test for hypothesis testing.

This statistical result confirmed that the implementation of cyber laws is successful in preventing cybercrime against women, and it resulted in rejecting the null hypothesis. According to respondents, the Information Technology Act of 2000's provisions and pertinent portions of the Indian Penal Code have helped to combat crimes including online harassment, cyber stalking, and sharing of images without consent. Nonetheless, the efficacy received a modest rating, indicating potential for improvement.

Evaluating the difficulties in putting cyber laws into practice for Delhi's women's safety was the second goal. The results showed a number of obstacles that lessen the regulations' possible influence. The absence of victim-friendly reporting procedures, court process delays, specialized cybercrime units, and insufficient technical infrastructure within law enforcement organisations were among the main problems. Furthermore, it was found that women's ignorance and social shame were major barriers to reporting events, which limited the potential for legal action. These difficulties show how legislative purpose and actual enforcement differ. The third goal was to make strategic suggestions for bolstering Delhi's cyber law enforcement in the fight against crimes against women. In light of the results, the study recommends a multifaceted strategy:

1. **Increased public understanding** of women's rights and accessible legal

remedies through focused digital literacy programs.

2. **The building of specialized cybercrime** investigative teams, frequent training, and the provision of cutting-edge cyber forensic technologies to law enforcement authorities.

3. **Streamlined legal procedures** to ensure timely investigation and prosecution, possibly through the introduction of fast-track courts for cybercrime cases.

4. **Victim support systems** such as confidential helplines, online complaint portals, and counseling services to encourage reporting and reduce trauma.

5. **Inter-agency collaboration** between police, judiciary, and cyber experts to improve investigation efficiency.

In conclusion, this study shows that although Delhi's cyber laws are largely successful in combating crimes against women, the present framework has to be strengthened to close implementation gaps. The null hypothesis' rejection affirms that enforcement has a significant impact, while structural changes, resource distribution, and public participation all have a significant impact on how successful enforcement is. To make the internet a safer place for women, legislators, law enforcement, civic society, and the general public must work together. In order to tackle cybercrime against women in India, Delhi can set an example by tackling issues that are both structural and awareness-related.

REFERENCES

1. Ahlawat (2024). India's cybercrimes against women. *Journal of Visual and Performing Arts, ShodhKosh, 5(6)*. https://doi.org/10.29121/shodhkosh.v5.i6.2024.2430

2. Choudhary, R. (2022). Cyberspace and Women- Dimensions of Cybercrime against Women in India. *Design Engineering (Toronto)*, 73–80. https://doi.org/10.17762/de.vol2022iss1.8685

3. Cooper, D. R., & Schindler, P. S. (2019). *Business research methods* (13th ed.). McGraw-Hill Education

4. Cresswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

5. Dar, S. A., & Nagrath, D. (2022). Are Indian women a prime target for cybercrime? *Journal of Computing and Information Technology, 3(1), 23–31*. https://doi.org/10.48185/jitc.v3i1.503

6. Dubey, S. (2021). *A Viewpoint on Women's Victimisation of Cybercrimes and Cyber Laws, 643–647*. https://doi.org/10.48175/IJARSCT-1443

7. Gribetz, S. K. (2022). Indian Women's Cybercrimes: How Can Technology and the Law Assist the Victims? *(pages 85-93). Hall/CRC and Chapman eBooks.* https://doi.org/10.1201/9781003204862-7

8. Halder, D. (2015). Women being victimised by cyberstalking: Assessing the efficacy of India's present legal framework from the viewpoints of therapeutic jurisprudence and restorative justice. *Temida, 18, 103–130*. https://doi.org/10.2298/TEM1504103H

9. Kothari, C. R., & Garg, G. (2019). *Research methodology: Methods and techniques* (4th ed.). New Age International Publishers.

10. Misra, R. (2013). Cyber Crime Against Women. *Social Science Research Network*. https://doi.org/10.2139/SSRN.2486125

11. Thangamayan, S. (2023). Cyber Crime and Cyber Law's In India: A Comprehensive Study with Special Reference to Information Technology. *International Journal on Recent and Innovation Trends in Computing and Communication*. https://doi.org/10.17762/ijritcc.v11i9.9379