INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBER CRIME AGAINST WOMEN IN INDIA

AUTHOR - RIYA DUBEY* & DR. SUKRITI YADAV**

* STUDENT AT AMITY UNIVERSITY LUCKNOW

** ASSISTANT PROFESSOR AT AMITY UNIVERSITY LUCKNOW

BEST CITATION – RIYA DUBEY & DR. SUKRITI YADAV**,** CYBER CRIME AGAINST WOMEN IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (6) OF 2026, PG. 513-517, APIS – 3920 – 0001 & ISSN - 2583-2344

CHAPTER 1 - INTRODUCTION

1.1 Research Background

The swift progress of information and communication technology has substantially transformed contemporary society. In today's world internet is essential for everyone, enabling communication, education, commerce, governance, and entertainment. With the proliferation of smartphones and the expansion of digital connectivity, millions of individuals across the world are now connected through different online platforms. In India, the digital revolution has accelerated with initiatives promoting digital infrastructure and online services. While these developments have enhanced opportunities and accessibility, they have simultaneously given rise to a new category of criminal activities commonly referred to as cybercrime.

Cybercrime is committing unlawful acts using computers, digital devices, or the internet . These crimes may involve unauthorized access to computer systems, identity theft, data breaches, cyberstalking, online fraud, and digital harassment. Unlike traditional crimes, cybercrimes are often characterized by anonymity, speed, and the ability to transcend geographical boundaries, making detection and enforcement more complex.

Among the different victims of cybercrime, women represent one of the most vulnerable groups in digital spaces. The growing use of social media platforms, online communication tools, and digital content sharing has unfortunately exposed women to many forms of online abuse and exploitation. Cyber harassment, cyberstalking, morphing of images, circulation of obscene content, and the non-consensual sharing of personal photographs or videos have become increasingly prevalent forms of cyber offences targeting women.

These forms of cyber violence often extend beyond mere technological misuse and constitute grave violations of a woman's dignity, privacy, and personal security. The effect of such offences is not limited to online platforms but often affects victims' social relationships, mental health, and professional lives. Many victims experience anxiety, fear, humiliation, and reputational harm due to the widespread circulation of offensive or manipulated content on the internet.

The issue is particularly concerning in the Indian context where social and cultural factors may discourage women from reporting cyber offences. Victims hesitate to report offences to enforcement authorities due to social stigma, lack of awareness about legal remedies, or lack of trust in investigative mechanisms. As a result, most of the cybercrime against women remain unreported, creating a gap between the actual prevalence of such crimes and the number of officially recorded cases.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Recognizing the seriousness of cyber offences, the Indian legal system has implemented different legislative measures to address cybercrime. The IT act 2000, provides legal remedies against different forms of cyber misconduct. These laws criminalize acts such as identity theft, violation of privacy, publication of obscene content, and cyberstalking. Furthermore, specialized cybercrime cells and digital forensic units have been established to investigate such offences.

Despite these legal provisions, the effectiveness of current laws in preventing cybercrime against women continues to be a matter of debate. swift technological developments, lack of digital awareness, and limitations in law enforcement capacity often hinder the efficient implementation of cyber laws. Therefore, it becomes essential to analyze the nature of cybercrime against women, evaluate the current legal framework, and identify potential reforms to strengthen digital safety.

This research seeks to analyze cybercrime against women in India from a legal perspective. It focuses especially on forms of online abuse such as harassment, stalking, morphing, and non-consensual sharing of digital content. By examining legal provisions, judicial decisions, and the practical challenges faced in addressing such crimes, the research seeks to provide a better insight on the issue and suggest possible improvements in the legal and institutional framework.

1.2 Literature Review

Cybercrime has emerged as a significant area of concern in legal scholarship and policy discussions. different researchers, legal scholars, and institutions have analyzed the phenomenon of cybercrime and its implications for individuals and society. In recent years, particular attention has been given to the issue of cybercrime against women due to the growing number of incidents reported across digital platforms.

Scholars studying cyber law have emphasized that the anonymity and accessibility provided by the internet create opportunities for individuals to engage in harmful activities without immediate accountability. According to several studies, cyberstalking and online harassment are among the most common forms of cybercrime experienced by women. These offences often involve sending threatening messages, monitoring online activities, spreading defamatory content, or repeatedly contacting individuals through digital platforms.

Academic research also highlights the role of social media in enabling cyber harassment. Platforms that allow users to create anonymous profiles and share multimedia content may sometimes be misused to spread offensive or manipulated material. Instances of image morphing, fake profile creation, and revenge pornography have raised grave concerns regarding online safety and digital ethics.

Legal scholars have also examined the effectiveness of current legislation in addressing cybercrime. The IT Act, 2000 is considered the foremost law governing cyber activities. Researchers have analyzed provisions related to privacy violations, identity theft, and the publication of obscene content. However, several scholars have argued that the law requires periodic updates to address emerging forms of cyber offences.

In addition to statutory provisions, judicial decisions have played a significant role in shaping cyber law jurisprudence in India. Courts have interpreted legal provisions relating to online speech, privacy, and digital offences in different landmark cases. For example, the judgement in Shreya Singhal v. Union of India substantially impacted the regulation of online speech.

Another area explored in academic literature concerns the psychological and social consequences of cybercrime against women. Studies indicate that victims often suffer from emotional distress, social isolation, and

reputational damage as a result of online harassment. Such experiences may discourage women from participating actively in digital spaces, thereby limiting their freedom of expression and access to information.

Despite the growing body of literature on cybercrime, there remains a need for more comprehensive research focusing specifically on cyber offences targeting women in India. current studies often highlight legal provisions but may not fully address the practical challenges faced by victims and law enforcement authorities. This research seeks to bridge that gap by analyzing both the legal framework and the real-world implications of cybercrime against women.

1.3 Objective research

1. To analyze the concept and nature of cybercrime against women in India.
2. To identify and analyze different types of cyber offences targeting women, including cyberstalking, morphing, and non-consensual sharing of digital content.
3. To research judicial interpretations and landmark cases related to cybercrime against women.
4. To evaluate the challenges faced by victims and law enforcement authorities in addressing cyber offences.
5. To suggest measures and policy recommendations for improving legal protection and digital safety for women.

1.4 Research Methodology

This research adopts a doctrinal research methodology, involving the analysis and interpretation of current legal materials. Doctrinal research focuses on examining statutes, judicial decisions, legal principles, and academic commentary in order to understand the development and application of law in a particular area.

The research relies predominantly on secondary sources of data, including books, academic journals, legal commentaries, government reports, and online legal databases.

Relevant statutory provisions contained in the Information Technology Act, 2000 and the Indian Penal Code have been examined in detail to understand the legal framework governing cybercrime.

Judicial decisions delivered by different courts in India have also been analyzed in order to understand how the judiciary interprets and applies cyber laws in cases involving offences against women. Landmark cases have been studied to evaluate the effectiveness of legal remedies and the evolving judicial approach towards cyber offences.

In addition to legal materials, reports and publications by governmental and non-governmental organizations have been consulted to understand the social effect and prevalence of cybercrime against women. These sources offer valuable insights into the patterns of cyber offences and the challenges faced in combating them.

The doctrinal approach allows for a comprehensive analysis of legal provisions and their practical implications. By examining statutory laws, judicial interpretations, and scholarly opinions, the research seeks to offer a critical understanding of the legal mechanisms available to address cybercrime against women in India.

Conclusion

The swift growth of cyber technology and the growing reliance on the internet have transformed contemporary society in many ways. Online platforms have created new opportunities for communication, education and business. However, along with these benefits, the digital environment has also become a space where different forms of crime can occur. Among these, cybercrime against women has emerged as a grave concern that

demands immediate action from lawmakers, law enforcement authorities, and social system at large.

This dissertation titled "Cybercrime Against Women in India: A Legal Analysis with Special Reference to Online Harassment, Morphing, Stalking, and Non-Consensual Email Sharing" aimed to analyze the nature, causes, and legal responses to cyber offences targeting women in India. Through an analysis of legal provisions, scholarly literature, case laws, and available statistical data, the research sought to evaluate the effectiveness of current laws and identify the challenges faced in preventing and addressing such crimes.

The research shows that cybercrime against women has increased substantially in recent years due to the swift expansion of internet usage and social media platforms. Digital technologies allow individuals to communicate instantly and share information globally, but they also offer opportunities for misuse. Women frequently become victims of online harassment, cyberstalking, image morphing, and the unauthorized sharing of personal information. These offences not only violate the privacy of victims but also have severe psychological and social consequences.

One of the significant findings of this research is that cybercrime often occurs due to the anonymity provided by digital platforms. Offenders can easily create fake identities and operate from unknown locations, making it difficult to trace them. This anonymity encourages individuals to engage in harmful behavior without fear of immediate consequences. Furthermore, the transnational nature of cybercrime creates additional challenges for law enforcement authorities, as offenders may operate from jurisdictions outside India.

Although these legal provisions offer a framework for addressing cybercrime, the research indicates that their implementation remains a challenge. Many victims are unaware of the legal remedies available to them, and in some cases, law enforcement authorities may lack the technical expertise required to investigate cyber offences effectively. Underreporting of cybercrime cases is another major issue, as victims often hesitate to approach authorities due to fear of social stigma or concerns about their privacy.

Another significant aspect highlighted in this research is the role of social media platforms and digital service providers. While these platforms have implemented policies to prevent harassment and abusive behavior, their enforcement is not always consistent. Victims sometimes face delays in getting harmful content removed, and reporting mechanisms may not always lead to immediate action. Therefore, greater accountability and cooperation from technology companies are essential to ensure the safety of users.

The research also emphasizes the importance of awareness and education in preventing cybercrime against women. Many incidents occur due to a lack of knowledge about online safety and privacy protection. Promoting digital literacy and educating individuals about responsible internet usage can substantially reduce the risk of cyber offences. Educational institutions, government agencies, and civil society organizations should work together to spread awareness about cyber safety and the legal remedies available to victims.

Furthermore, strengthening law enforcement mechanisms is crucial for effectively addressing cybercrime. Specialized cybercrime investigation units, improved digital forensic capabilities, and regular training programs for police officers can enhance the ability of authorities to investigate and prosecute offenders. Victim support services, including legal assistance and counseling, should also be made more accessible to ensure that victims receive adequate support during the legal process.

The recommendations provided in this dissertation aim to create a comprehensive strategy for addressing cybercrime against

women. Strengthening legal provisions, improving enforcement mechanisms, promoting awareness, and encouraging responsible digital behavior are essential steps toward ensuring a safer online environment.

In conclusion, cybercrime against women is a complex issue that requires a coordinated response from multiple stakeholders. Governments, law enforcement agencies, technology companies, educational institutions, and society must work together to combat cyber offences and protect the rights and dignity of women in the digital space. Ensuring the safety of women online is not only a legal obligation but also a fundamental step toward achieving gender equality and social justice in the contemporary digital world.

As technology continues to evolve, it is essential for laws and policies to adapt accordingly. Continuous research, policy reforms, and international cooperation will play an significant role in addressing emerging forms of cybercrime. By implementing effective preventive measures and strengthening legal protections, it is possible to create a digital environment where women can participate freely and confidently without fear of harassment or exploitation.

Ultimately, safeguarding women from cybercrime is essential for building a just and inclusive society in which technological progress benefits all members of the community.