IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

# CYBERCRIME AGAINST WOMEN: AN ANALYSIS OF LAWS AND THEIR EFFECTIVENESS IN INDIA

**[1]Sowmiya, [2]Dr. Aswathi Sukumaran,**

[1]Student, [2]Assistant Professor,
Department of Law,
Vels Institute of Science, Technology & Advanced Studies,
VISTAS,
Pallavaram, Chennai - 600117, India

**ABSTRACT:** The rise in the number of cybernetic crimes against women has made cyber crime, in general, an issue of growing concern. Cyber crimes against women via cyberspace include but are not limited to, stalking, harassment, identity theft, and the posting, without the consent of the victim, of nude or sexually explicit images of another individual. The study concentrate on doctrinal research which examine the law of the cyber crime against women in India under both the Information Technology Act 2000 and the Indian Penal Code 1860 as they pertain to all of the above-mentioned offences. In addition to providing an overview of the various provisions of the above-mentioned Acts, the analysis will assess whether each law is effective and will make suggestions for legal reform where necessary.

**Index Terms-** Cybercrime against women, Non-consensual image sharing,Women's rights in cyberspace

## I. INTRODUCTION

The development of technology has greatly changed communication, social interaction, and information gathering in the current society. The emergence of internet services, social networking sites, and digital devices has brought new ways to help grow and develop. Nevertheless, together with these advantages, cybercrime has increased at a fast pace, raising many problems. Cybercrime includes different offences that have brought great concern, and one among those is cybercrimes against women, as a result of abuse of technological advancement. Women are now facing cyberstalking, harassment, identity fraud, image morphing, and dissemination of their private and intimate material without their consent. Such offences not only infringe upon their rights, but they also affect their dignity and privacy. The single factor which distinguishes cybercrime from all others is the anonymity factor in which the offender carries out the crime without revealing his/her identity. It becomes quite difficult for any law enforcement agencies to trace these offenders and act upon them owing to the nature of anonymity offered by the internet. Further, the absence of limits in the virtual world also causes difficulty for law enforcement agencies to conduct their investigation and hold the culprit responsible for his/ her actions. The impact of cybercrime on women cannot be limited to the virtual environment as its impact is felt psychologically, emotionally, socially, and personally. The legal framework regulating cyber crime in India mainly includes the Information Technology Act, 2000 and the Indian Penal Code, 1860. Under these acts, there are specific provisions which deal with crimes against electronic communication, obscenity, harassment, and data abuse. However, these acts were passed when cyber crime was still in its infancy, and technology was not so developed. The emergence of new technology-based cyber crime offences requires new laws which have not been passed yet. The question arises whether the existing legal framework is sufficient for dealing with cyber crime against women. It therefore becomes important to analyse the provisions made legally, find any loopholes within the existing provision, and analyse the difficulties in its implementation. It is necessary to have a

clear knowledge of the problems mentioned above to ensure that the law continues to be relevant in safeguarding women from being victims of cybercrime in cyberspace. This paper attempts to study whether the present laws pertaining to the protection of women from cybercrime are adequate.

## II. CONCEPT AND NATURE OF CYBERCRIME AGAINST WOMEN

Cybercrime against women is defined as crimes committed by perpetrators online specifically targeting women using the internet (the world wide web). Examples of the types of cybercrimes committed against women include cyberstalking, online harassment, cyberbullying, morphing of images or video or photographs, identity theft, and the non-consensual sharing/dissemination of intimate content or photos. All of these acts violate legal rights and also violate the dignity and privacy of women.The characteristic feature of cybercrime is that it changes and develops in tandem with developments in technology. Unlike conventional criminal activity, where it is possible to pinpoint perpetrators of crime because of their physical presence at the scene, cybercrime can be committed virtually without revealing one's identity. This adds complexity to legal action and makes cybercrime unique.

## III. LEGAL FRAMEWORK IN INDIA

### A. INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 is the main statute in India that regulates cyber crimes and serves as the basis for regulating electronic communication and transactions. The Act was passed to aid e-commerce transactions and provide legal status to electronic documents and digital signatures. However, the Act also helps to tackle cyber crimes. The Act has sections on computer-related offences like hacking, illegal access to a computer system, impersonation, data theft, and publishing obscene material electronically. Section 66 of the Act talks about computer-related offences and punishes offences like illegally or dishonestly accessing a computer system, damaging data, and disrupting computer functions. This section is commonly used to prosecute hacking and unauthorised access to an individual's account, which could adversely impact women since they might have private details in their accounts. Another important clause is Clause 67, which provides punishment for any publication or transmission of obscene matter through any electronic medium. This clause becomes extremely relevant if we take into consideration the problems related to the distribution of sexually explicit matter, such as the non-consensual distribution of sexually explicit images of women. Furthermore, Section 67A and 67B relate to even more serious types of matter, such as sexually explicit matter and matter relating to children. The purpose of this section is to make sure that digital media are not used as mediums of exploitation and harassment, particularly against women. In spite of its importance, however, there are some weaknesses of the Act when it comes to tackling issues related to cybercrime against women. To begin with, it does not mention any offences related to cyberstalking, online harassment, or image-based abuse. Consequently, the enforcement officers tend to refer to the broad wording of the Act, which cannot reflect the severity of the situation. Additionally, with technology developing very fast, new types of cybercrimes have been invented; these include, for example, deepfake content or online trolling. Thus, the Act seems to be incomplete in this respect. The other difficulty comes in terms of interpreting and implementing the Act. There may be ambiguities in the implementation of the Act because it lacks a clear definition of certain terms. Moreover, it may prove difficult for the implementing body to conduct investigations into cyber-crimes owing to the technological nature of such crimes. It can be concluded that while the Information Technology Act, 2000 provides the basic structure for tackling cybercrimes in India, amendments are necessary to update the Act.

### B. INDIAN PENAL CODE, 1860

The Indian Penal Code, 1860 can be viewed as a vital complementary measure for tackling cyber crimes against women in India when the provisions made under cyber law fall short of tackling them. While the enactment of the Indian Penal Code took place long before the development of computers and internet, the vast majority of its provisions have been used for crimes committed using these technologies. Some of the key provisions under the Indian Penal Code include stalking, criminal intimidation, defamation, and offences to the honour and integrity of women among others. For example, provisions pertaining to stalking have commonly been used in cases of cyber-stalking, whereby a person continuously contacts or watches women over social media sites or any other online platform. Moreover, the IPC contains provisions related to criminal intimidation, which can apply when women are intimidated in cyberspace through e-mails, messages, or social networking websites. In cases where women suffer from defamation, which is an offence committed using any medium, including cyberspace, the laws of defamation under the IPC are applicable. Such laws can deal with a variety of offences committed in cyberspace but not specifically mentioned under

cyber laws. Besides, other offences like identity theft and impersonation, when not covered by cyber laws, can be tackled using general laws like cheating and fraud under the IPC. However, there are various shortcomings associated with the Indian Penal Code that makes it difficult for the law to be effective in preventing cyber-crimes against women. One of the major shortcomings of the Indian Penal Code is that it lacks any provision intended to prevent cyber-crime. The absence of any special provision in the Indian Penal Code makes it quite hard to determine how various provisions in the code can effectively address the issue of cybercrime. Failure of the Indian Penal Code to explain what is meant by terms like cyberstalking and cyber harassment complicates the interpretation of provisions in the act. One more important aspect that needs consideration is that there is no system within the IPC for handling such issues as the rapid dissemination of information through the Internet and instant data deletion. Unlike the cyber laws, where the focus is on preventing and addressing the issue at the platform level, this is not true in the case of IPC. Therefore, even though IPC, 1860 will play a critical role in dealing with cybercrimes committed against women, it alone will not be able to achieve the objective.

## C. OTHER RELEVANT LEGAL PROVISIONS

In India, apart from the Information Technology Act, 2000 and Indian Penal Code, 1860, there are other major legislation concerning privacy and data protection that have an essential role in combating cyber crimes perpetrated against women. With the advent of the Internet, people tend to reveal their personal information such as images, videos, personal information, and financial information, making them very private. The use of this information without the owner's consent leads to a great possibility of cyber crimes. It is worth noting that women are the primary targets for most cyber crimes such as identity fraud, harassment, stalking, and uploading personal photographs without the owner's consent. One significant principle established within this structure is that through Article 21 of India's Constitution, establishing the right to privacy as a fundamental right through a judicial finding made by the Supreme Court in Justice KS Puttaswamy v. Union of India, establishing the right to privacy as an integral part of the right to life and liberty. The relevance of this ruling concerning cyber crimes is that it creates a constitutional protection for individuals against violations of their right to privacy due to cyber crimes. Privacy issues have only become more pressing when taken into account with the continued abuse of women's privacy through incidents such as the distribution of intimate photographs posted on social media without consent. Apart from the constitution, some provisions in the IT Act also provide for data protection to some extent. Section 43A of the IT Act makes it mandatory for companies and other bodies to ensure the safety of the sensitive personal data and to be liable for any wrongful loss or gain arising out of their failure to ensure the same. It aims at prompting organisations to adopt proper security measures regarding users' data. Yet, the ambit of the provision remains restricted and applies mostly to corporations rather than the offenders themselves. The country has made some progress towards formulating an inclusive data protection law as well, as seen from the enactment of the Digital Personal Data Protection Act, 2023. Such laws aim at regulating the processes of collecting, using, storing, and processing personal data to give more powers to people regarding their data. Such concepts like consent, minimisation, and accountability of data fiduciaries have been introduced by the law. These concepts play a major role in dealing with cybercrimes that are committed owing to the abuse of personal data. Nevertheless, given that the law has just been implemented, its potential impact on cybercrime against women can be evaluated later on. However, even amidst all these progressions, there are considerable shortcomings present within the legal system as regards data protection laws and privacy in India. The primary challenge lies in the fact that there is no specific law that clearly and comprehensively addresses the problem of abuse of data within cyber crimes. There is also an absence of adequate enforcement within the system along with low awareness levels among the citizens about data protection issues. Technological changes have also resulted in the emergence of several challenges such as data breach, surveillance, and profiling. Even though certain legislative measures and constitutional principles exist in India, these are not enough to cater to the issue of cybercrime against women due to its complexities. The enforcement of legislation related to data security along with increasing user awareness, constant amendments in law, etc., will play an important part in ensuring privacy and protection of the data of individuals. In this regard, it can be said that privacy and data protection have a significant role in stopping cybercrime against women.

## IV. ROLE OF INTERMEDIARIES AND PLATFORM REGULATION

The role played by intermediaries is essential to the digital environment, and it has great influence over the dissemination and management of cybercrimes against women. An intermediary refers to social media sites, websites, messaging software, internet service providers, and other online networks that enable people to communicate and share information between each other. The platform acts as the medium through which individuals generate and distribute information. As much as it offers opportunities for interaction, it also enables individuals to commit cybercrimes including cyberbullying, stalking, and the distribution of personal images without consent. Given that cybercrimes against women are largely executed using these platforms, their importance is great. In terms of Information Technology Act, 2000, the intermediaries are offered safe harbour protection. The intermediaries will not be held responsible for the contents posted by third parties on their platforms as long as they remain neutral and refrain from being active in creating and modifying the content posted thereon. But, it is not an unconditional protection for intermediaries. There are some conditions attached to this protection that need to be fulfilled before intermediaries can avail themselves of this exemption from liability. One of the conditions is that intermediaries have to act responsibly. This is among the responsibilities of the intermediaries as per their mandate to either delete or block access to illegal material once there has been notification or actual knowledge to this effect by any authority or person aggrieved by the same. This is particularly relevant in cases where a crime has been committed against a woman through the internet because the content which may entail threats, defamation or even private images can spread fast and lead to irreparable damage. In recent years, the framework governing regulations has also been enhanced in order to improve accountability on the part of the intermediaries. Regulations on intermediary guidelines mandate the establishment of grievance redressal systems, compliance officers, and timely responses to complaints. This is done to ensure that the victimised party is accorded justice and their complaint is addressed in a timely manner. For cases involving women victims of cyber crimes, it becomes easier for them to report the crime and remove any harmful material from the platform.

## V. CHALLENGES IN ADDRESSING CYBERCRIME AGAINST WOMEN

Even though there are laws made in the Information Technology Act, 2000, and the Indian Penal Code, 1860, there have been several issues which pose problems in dealing with cybercrimes committed against women. The foremost among these is anonymity and untraceability of perpetrators. Cyber criminals tend to protect themselves by using false identities on fake email addresses, virtual private networks, and encryption services, making the prosecution process very tough for law enforcement authorities.Another major problem concerns the insufficient provision under the laws currently available. In the case of the IT Act of 2000, there is no provision for any emerging cybercrime such as cyber-stalking, bullying, deepfake pornography, and image based abuse. Therefore, it becomes difficult to prosecute individuals as the crimes fall into general or outdated provisions that cannot possibly be reflective enough of the crime involved. Another problem that stems from the issue of jurisdiction lies in the unavailability of an address because of cyberspace. These cybercrimes can be carried out across many jurisdictions making it challenging for authorities to investigate, collect and prosecute evidence. Another major problem pertains to the lack of technological know-how among authorities.The other issue facing cybercrime against women is the underreporting of the crime. This can be attributed to various factors like social stigma, fear of retaliation, ignorance about the legal system, and even the lack of trust on the part of the victims in the process and its outcomes. This makes most of the offenses committed in cyberspace go unnoticed. Delayed investigations and trials make the use of law less effective since cybercrimes require prompt actions. Lastly, lack of awareness by users regarding how to protect themselves in cyberspace leaves them vulnerable to attackers in cyberspace.

## VI. SUGGESTIONS AND LEGAL REFORMS

In order to combat cybercrime against women, there needs to be a multifaceted approach that would entail changing laws and societal structures. The first step would be to make changes to the existing provisions of the Information Technology Act, 2000 and include such things like cyberstalking, cyber harassment, use of deepfakes, and non-consensual sharing of private photos as criminal offenses. Next, there needs to be cybercrime units in all states which would have adequately trained people and advanced technology and also have sufficient funding.Thirdly, the government can facilitate speedy trial of cases pertaining to cybercrimes especially those where women are involved so that victims do not face unnecessary delays leading to increased trauma. It is also imperative to improve the accountability of intermediaries. This can be achieved by increasing the process of monitoring content on social networking websites, introducing swift mechanisms of redressal of grievances, and detecting any content that might be

abusive or threatening, for example, deepfakes. Moreover, international cooperation can be sought in investigating cybercrimes via various treaties and collaborations.Initiate a drive that will enable women to learn about their rights when it comes to their personal internet security, their right to privacy, and seeking legal support if they have been made victims. This kind of educational training can be integrated into already existing courses on the internet in schools. Apart from ensuring that there is an educational curriculum that ensures that women use the internet in a safer way, setting up victim assistance programs such as counseling and legal aid will ensure that there are fewer victims who suffer emotionally from being a victim.

## VII. CONCLUSION

Cybercrime targeting women is a significant and constantly developing issue in the modern technological age that knows no borders or conventional crimes. While the world is becoming increasingly digitized through technology used in communication and business, women are also becoming increasingly vulnerable to cyber crimes in terms of exploitation and harassment, as well as invasion of their privacy. The effect of such crimes goes beyond violating the law and extends into the psyche of women.A study of the current legal system in India demonstrates that although the IT Act, 2000, and the Indian Penal Code, 1860, form the basic structure for dealing with cyber crimes, they fail to cope up with the intricacies involved in the recent forms of cyber crime. There is no provision in the existing laws to counter issues related to cyberstalking, deepfake technology, and the unauthorized circulation of explicit photographs or videos without the consent of the individual.The acknowledgment of the right to privacy as a basic right and the passing of the Digital Personal Data Protection Act, 2023 are significant steps in building the legal framework. Nevertheless, the mere establishment of legal provisions without implementing and enforcing them effectively, together with issues related to anonymity, jurisdictions, lack of skills, and under-reporting, will remain a barrier to its success. However, it is also clear that cybercrime directed towards women will not be solved through punitive laws alone. It is important to have a preventive strategy for dealing with victims, where there needs to be an early detection system. There also should be the removal of harmful content within the shortest possible time from the Internet.The law must evolve along with it. Updating legislation, policies, and even interpretations from courts become inevitable in order to stay ahead of any new technology that may come up. It is important for all stakeholders, including the government, police, tech firms, and civil society, to work together. Combating cybercrimes committed against women cannot be limited merely to a criminal justice matter, but is rather an act of social responsibility. Besides promoting positive attitudes, there should be new approaches to thinking in terms of digital ethics, gender sensitivity, and proper conduct online. Through educating women about their rights in Internet usage, we can successfully deter such cybercrimes and provide help for them as well.In conclusion, although India has made remarkable progress in terms of legislation and constitution, there are certain areas where there is no proper solution to protect women from the threats of cyber-crime. Multiple solutions need to be implemented simultaneously to create a secure virtual environment where everyone can participate without fear. There is no alternative way left to safeguard women from cyber-crime other than a consistent effort in multiple dimensions.