*Page 485 - 498* **DOI:** *https://doij.org/10.10000/IJLMH.118553*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 7 | Issue 6**

**2024**

# Empowering Women against Cyber Crime: Legal Deficiencies and The Need for Reform in India

RAJVEER SINGH RATHORE[1] AND DR. NAVNEET CHAHAL[2]

## ABSTRACT

*Cybercrimes against women are increasing and women have been severely victimized in cyberspace. Some criminals try to offend women by sending obscene e-mails, stalking women through chat rooms, websites, etc., developing pornographic videos that present women in compromise, mostly created without their consent, fraudulent e-mails, images that turn into pornographic content, etc. Sex offenders look for their victims on social networking sites as well as job or matrimonial sites where people post their personal information for a better future. Disclosure of personal information has made women increasingly victims of cybercrime. Although there are many cases of female victimization in western countries, female victimization has increased in eastern regions such as India, and these women have relatively less legal protection and are unique than their western counterparts (Halder and Jaishankar), 2008, 2009, 2011b). This article attempts to explore the various reasons why Indian women have been victimized and proposes a conceptual model of Indians women cyber victimization. As victims of cybercrime, women experience a number of psychological effects that deeply affect their lives. The National Crime Records Bureau (NCRB) has reported an increase in cybercrimes against women in recent years. Cybercrime against women takes the form of online defamation, sexual harassment and abuse, email spoofing, etc. This research paper is an attempt to discuss a brief analysis of women legal rights to protect themselves against cybercrime, its implementation and the challenges women face in achieving these rights.*

***Keywords****: Cybercrime, Regulations, Law and Policy, IT Act 2000, Technology*.

## I. INTRODUCTION

Cybercrime is a global phenomenon. Women have been victims of various types of harassment for centuries and until now. Domestic violence, Sathi Paratha, acid attack, rape, bullying, sexual harassment, dowry, harassment, kidnapping, honour killings, female infanticide, etc. are some of the categories of violence against women. The brutal rape death of a 23-year-old paramedic

[1] Author is a LL.M. Student at UILS, Chandigarh University, Mohali, Punjab, India.
[2] Author is a Head of Department at UILS, Chandigarh University, Mohali, Punjab, India.

 [ISSN 2581-5369]

in New Delhi last December drew attention to violence against women and for the first time sparked widespread protests among Indians across the country who raised their hands against the violence. against women in India. The United Nations defines violence against women as any gender-based violence that causes or may cause physical, sexual or mental harm or suffering to women, including the threat of such acts, coercion or arbitrary deprivation.

Acc. to Swapna Majumdar: "Violence against women is not cultural or regional; it involves community and class. Although shocking, the fact is that violence against women has become an accepted norm of life because women accept violence as part of their marriage until it becomes intolerable. (Majumdar 2003). We all celebrate International Women's Day every year on March 8 to show our respect, love, affection and appreciation to women for their economic, political and social achievements in various fields. Even in India women are worshiped as goddesses (Devi), Kanya, Mata etc.) but the reality shows a darker and deteriorating picture of it. Actually, women are worshiped only in religious places or religious programs or festivals but in common life they are used in many ways and always were victims of physical, psychological, sexual abuse etc. India has become the worst place in the world for exploitation of women. It feels proud because it is considered the world's largest democracy, but the recent gang rape of a woman running in a bus in Delhi, abuse of a woman, dowry harassment, dowry death, harassment, kidnapping, domestic violence, female infanticide, honour killings. cyber violence etc. reveal the true picture of India, how difficult it is for women life in Indian democracy. Equality of all was mentioned in the preamble of Indian constitution e.g. "To secure to all its citizens social, economic and political justice, freedom of thought, speech, religion, belief and worship; equality of status and opportunity; fraternity that guarantees the dignity of the individual and the unity of the people. In the aforementioned law, certain crimes are classified as punishable crimes, such as hacking, publishing obscene material online, data manipulation. Safe environment offers to parents to improve their children's online safety. Both technical measures to protect computer systems and legal measures to prevent and prevent crime are implemented. Cyberspace is a new horizon driven by machine data and any criminal activity that uses a computer or network as a source, tool or target is called cybercrime.[3] Cybercrime against women in India is a new concept. When India started its IT journey, the protection of e-commerce and communications under the Information Technology Act, 2000 was paramount, while cyber-data communications remained untouched. It used to be limited to roads or places away from home. Home was the safest place for a woman to protect herself from victimization,

[3]Karuppannan Jaishankar and Puthisigamani Kosalai, "Victims of stalking in India: A study of girl college students in Tirunelveli City,"10 *Temida* 13 (2007).

 [ISSN 2581-5369]

but not now. Home becomes for them an equally dangerous place, prone to criminals. However, the limit will be set on their computer screens. This is a serious concern. The increase in cybercrimes against women has led to insecurity among women. They don't know nowhere is safe anymore. Its impact on them and society as a whole is greater when looking at the bigger picture.[4] Today, in this globalized world, we are surrounded by various man-made inventions our life is simple and comfortable. One such great invention of mankind is the Internet. From online shopping to collecting Due to the rapid development of the cyber world, information is now so easy and accessible. One can you can get information on any topic in minutes. Easy access to computers and things on the Internet is rapidly changing around us, from communicating with friends and family to studying and working online the feeling of home seems so accessible to all. It has become a part of our lives. Besides, we all are depend on internet for every little thing. Cybercrimes such as cyber terrorism, identity theft, it targets phishing emails, data breaches, privacy breaches, fraud and other computer-related crimes.

## II. CONCEPT OF CYBERCRIME

The industrial revolution opened the way to modernization and technological development. Together as technology has evolved over time, it has gradually changed the settings of the entire society. But the biggest cyber development contributed by the INTERNET. It has become part of our daily needs. But eventually it became a platform to commit crimes. People started abusing this great invention. The development of the Internet in the cyber world brought a drastic change in the modernization of the world, but even opened doors side effects This gave birth to what we now call "CYBERCRIME". Today every third person has been a victim of some sort of cyber abuse. It has spread its roots all over the world whether you talk about developed nation or underdeveloped nations. The cybercrime poses threat not only to individual but even to national security and the citizens of the nations. In the growing trend of using smart phones and being active on social media sites one must not forget that apart from being an entertainment platform, it poses a threat of cybercrime as well. But in most of the cases it is seen that the cyber criminals always look towards new methods to attack the individual either for his own interest or for the sake of entertainment. This can be done against anyone without even knowing that we have fallen victim to it. Like today, when everything is digitized, it changes it is easy for a criminal to target a person and commit a crime against them.

[4]Shobhna Jeet, "Cybercrime against women in India: Information Technology Act, 2000" *Elixir International Journal* 11(2012).

### (A) Objective of this study:

- To study the concept of cybercrime against women.
- Female insecurity increases cybercrime.
- View all laws regardless of whether traditional or modern technology means.
- To study the existing legislation on cybercrime in India and find out whether it exists are adequate to fight cybercrime or there are loopholes in existing laws
- To finds out the problems of women in reporting crime and other causes of crime fewer convictions for cybercrimes against women.
- Explain the steps regulatory agencies must take to analyse crime against women.
- Need for effective intelligence apparatus to fight cybercrime against women.

## III. TYES OF CYBERCRIME AGAINST WOMEN

Basically, cybercrime is any illegal activity that uses a computer as the main means of execution. It has been expanded to include activities such as crime on the Internet, crime related to the Internet, violation of Internet laws, illegal activity through the Internet, violation of the Internet Act, computer crime, violation of any law through the Internet. Internet, Internet corruption, Internet criminal activity, Internet malware, electronic crime, Internet crime, Internet smuggling, Internet stalking, Internet identity theft. Cybercrimes can be committed against persons, property and government. The most common types of cybercrimes are discussed below.

- **Email Bullying**: This is not a new concept. It is very similar to bullying. This includes blackmail, threats, harassment and even email fraud. Although e-bullying is similar to letter bullying, it often causes problems when sending fake IDs. Harassment includes blackmail, threats, harassment and email fraud. The Criminal Law Amendment (Bill) 2013 was recently drafted under the Indian Sexual Harassment Act. It defines harassment as physical contact and advances that include unwanted and explicit sexual overtures.

- **Cyber stalking**: This is the use of the Internet to abuse or harass someone online. A cyber stalker does not physically harm the victim, but monitors the victim's online activities to gather information. Uses verbal threats to threaten the victim. A study of 72 women by Megha Desai and K. Jaishankar found that 12.5% of those surveyed were intimate with their cyber stalker before the stalking began. The Ritu Kohli case was

 [ISSN 2581-5369]

India's first cybercrime case. In this case, Mrs. Ritu Kohli has complained to the police about a person using her identity to chat on the Internet, mostly on a Delhi channel, for four consecutive days. He also complained that the person chats online, uses a name and speaks obscene language. The same person also gave his phone number to other chatters and asked them to call Ritu Kohli. He received almost 40 calls from unknown numbers. The IP address was traced and the whole matter was investigated by the police and eventually the criminals were arrested. Section 72 of the Information Technology Act covers laws relating to cyber consequences. It says that the preparation can be ordered far admiring the modesty of the women.

- **Cyberpornography**: Cyberpornography refers to the use of cyberspace to create, display, distribute, import or publish pornographic or obscene material, especially material depicting sexual activity between children and adults. Cyber pornography is a crime classified as causing personal injury. A very famous case of DPS MMS scandal was reported under this type of cybercrime. In this case, an MMS clip was made by a schoolboy in a dangerous situation, which was distributed among different networks. In several other cases, video clips leaked through CCTV recordings are very popular. Section 67 of the IT Act, 2000 covers cases of cyber-porn. According to this law, the perpetrator of the act can be punished under a different section of the criminal code.

- Section 290 of IPC or Section 270 of BNS on public nuisance.

- Section 292 of IPC or Section 294 of BNS on obscene sale of books etc.

- Section 292A which deals with printing or publishing grossly indecent or malicious or deceptive material.

- Section 293 for sale of obscene articles to minors.

- Section 294 of IPC or Section 296 of BNS for making or composing, writing obscene songs etc. and

- Section 509 of IPC or Section 79 of BNS to outrage the modesty of women. Women are easy targets for any type of cybercrime. With more than 560 million Internet users, India is the second largest online market in the world after China, according to research. Studies have also reported that by 2020, 40% of women will use the Internet. Among the states of Kerala, Tamil Nadu and Delhi, the percentage of female internet users is higher. Expert reports have also said that cybercrimes against women, especially sexual harassment, have increased significantly during the COVID-19 lockdown, with

 [ISSN 2581-5369]

"cage criminals" targeting them online.

- **Cyber defamation**: Cybercrime including defamation, is another common online crime against women. This occurs when defamation is committed via computers and/or the Internet. For example, someone posts defamatory material on the website or sends emails containing defamatory information to all of that person's friends or relatives. This is mostly done by hacking someone's Id on Face Book, Google or any other social network or post office. This is also done by creating a fake profile of a person that contains all the personal information that looks authentic to others on any website.

- **Morphing**: Changing the original image by an unauthorized user or a false identity is called morphing. Fake users have been found uploading photos of women and reposting them on various websites, creating fake profiles after editing.

- **Email spoofing**: An email that misrepresents its origin is a fake email. That shows its origin different from the actual origin.

## IV. LEGAL FRAMEWORK FOR THE PREVENTION OF CYBERCRIME AGAINST WOMEN

The internet has two unique characteristics. Firstly, it transcends physical / geographical barriers, and hence, the abuser may be acting from any part of the world. Secondly, the internet extends anonymity to the users. Essentially; there are two major laws in India that address cybercrime against women to a large extent – The Indian Penal Code 1860, (Bhartiya Nyaya Sanhita 2023) and the Information Technology Act. The IPC is a general criminal law of the land, which defines a large number of offences, and prescribes punishment for the same. Unlike the BNS, the IT Act is a Specific Law dealing with the many aspects of the use of information technology, including the commission of crimes. Under the Information and Technology Act, 2000, stalkers and cybercriminals can be booked under several sections for breaching of privacy:

Section 66A: Sending offensive messages through communication service, causing annoyance etc., through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment up to three years or fine.

Section 66B: Dishonestly receiving stolen computer resource or communication device with punishment up to three years or one lakh rupees as fine or both.

Section 66C: Electronic signature or other identity theft like using others' password or

electronic signature etc.

Section 66D: Cheating by person on using computer resource or a communication device shall be punished with imprisonment of either description for a term which extends to three years and shall also be liable to fine which may extend to one lakh rupee.

Section 66E: Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both.

Section 66F: Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization.

Section 67 deals with publishing or transmitting obscene material in electronic form. The earlier section in ITA was later widened as per ITA Act, 2008 in which child pornography and retention of records by intermediaries were all included.

Section 72: Punishment for breaching privacy and confidentiality diaries were all included.

Section 354D: This section deals with stalking. It defines stalker as a man who follows a woman and tries to contact such woman, monitors every activity undertaken by the woman while using digital media.

## V. CONSTITUTIONAL LIABILITY

Gaining unauthorized access to another person's belongings or appropriating their creative work is a clear infringement of their right to privacy. The Indian constitution does not explicitly include the "Right to Privacy" as one of the Fundamental Rights granted to Indian citizens, but it is safeguarded under the IPC.

The right to property is a fundamental human need, establishing boundaries that restrict access to individuals. The right to privacy prevents any interference or intrusion into someone's private life. The Supreme Court of India has unequivocally confirmed in its legal rulings that the right to privacy is an integral component of the Fundamental right protected under Article 21 of the Indian Constitution.

Therefore, the right to property now falls within the expanded scope of Article 21 of the Indian Constitution. Whenever there is a case of cybercrime concerning a person's private property or personal belongings, the accused may face charges for violating article 21 of the Indian Constitution. Legal remedies can then be pursued against the accused. Sure! Just let me know the text you want me to rewrite in a smooth manner.

 [ISSN 2581-5369]

## VI. JUDICIAL APPROACH

**1. Ritu Kohli Case:** Ritu Kohli Case was India's first instance of cyberstalking. Ritu Kohli has brought to the attention of the authorities an incident involving someone who has been impersonating her online on the website http://www. micro. com/. This has been happening on the Delhi channel for four consecutive days. Mrs. Kohli expressed further dissatisfaction regarding the individual's chatting habits. Ritu Kohli Case represented India's inaugural incidence of cyber stalking. In this specific case, 11 individuals were involved. Mrs. Ritu Kohli has lodged a complaint with the police against an individual who has been impersonating her online on the website http://www. micro. com/. This has been taking place mainly in the Delhi channel for a period of four consecutive days. Mrs. Kohli expressed her concern about someone using her name and address on the internet, engaging in inappropriate chat conversations with obscene language. The individual was also intentionally sharing her phone number with other chat participants, urging them to contact Ritu Kohli at all hours. Consequently, Mrs. Kohli received almost 40 calls in three days, primarily concerning additional hours.

The call in question caused chaos in the complainant's personal life. As a result, IP addresses were traced, police conducted a thorough investigation, and the offender was ultimately apprehended. A case was registered under section 509 of the IPC, and he was subsequently released on bail. This marks the initial instance when a case of cyber stalking was brought to light. Similar to email harassment, cyber stalking is not addressed by the current cyber laws in India. It falls within the scope of Section 72 of the IT Act that an offender can be held accountable from a distance for violating confidentiality and privacy.
The accused may also face charges under Section 441 of the IPC for criminal trespass and Section 509 of the IPC for outraging the modesty of women.

**2. State of Tamil Nadu vs. Suhas Katti,** in this instance, emails were sent to the victim, a divorced woman, for information by the accused through a false email account created by him in her name. The victim experienced mental harassment due to receiving annoying phone calls as a result of messages being posted, thus causing distress. She consequently lodged a complaint in the Egmore court in February 2004 and the accused was apprehended by the cyber cell of the Chennai police. He was charged under Section 469/509 IPC and Section 67 of IT Act, 2000. Charges were proven against him, and he was then booked under the aforementioned sections. A case was reported from Kottayam in Kerala, where a girl went to meet a person, she had connected with on Facebook. When she encountered him, she was taken away. The girl was

eventually located. Later, she informed the Police that the boy had forcefully taken her to a hotel and assaulted her.[5]

## VII. LEGAL DEFICIENCIES

Many countries have laws addressing online crimes, yet legal systems often struggle to effectively protect women in cyberspace because of specific deficiencies. Let's delve into the main legal shortcomings in relation to cybercrimes against women.

### 1. Insufficient legislation and coverage gaps:

**Absence of Specific Laws:** Numerous jurisdictions lack specific legislation that addresses offenses such as cyberstalking, online harassment, or revenge porn. Current criminal laws often lack specificity and may not adequately address the distinct characteristics of cybercrimes.

**Ambiguity in definitions** can prove challenging within the realm of laws, particularly in cases involving offenses like cyber harassment or stalking. This lack of clarity can hinder courts in their efforts to interpret such laws with consistency.

### 2. Jurisdictional matters in international cybercrime:

**Dealing with Enforcement Challenges Across Borders:** Given the global nature of the internet, perpetrators and victims may be situated in different countries. This presents challenges in enforcement as a result of jurisdictional boundaries and a lack of global cooperation.

**Inconsistent International Laws:** Cybercrime laws vary greatly from one country to another, resulting in challenges in clearly defining and prosecuting cases of online harassment or abuse on a global scale.

**Challenges in Extradition:** Despite international laws being in agreement, extraditing cybercriminals is frequently intricate and time-consuming, ultimately resulting in delayed justice for numerous victims.

### 3. Challenges in Evidence collection and preservation:

**Digital Evidence Standards:** Cybercrimes involve digital evidence that can be challenging to collect and preserve. Various criteria for acceptable evidence can make the prosecution process more complicated.

**Data Protection and Privacy Laws:** Data privacy laws can limit the gathering of online evidence from social media or other platforms, creating challenges for investigations.

[5]*Tamil Nadu V. Suhas Kutt, 4680 of 2024 Criminal Complaint*.

 [ISSN 2581-5369]

**4. Challenges centred around victims in seeking legal recourse include:**

**Victim blaming and stigmatization:** Women who report cybercrimes frequently encounter societal judgment and scepticism, diminishing their likelihood of being treated seriously and discouraging them from pursuing legal avenues. Legal systems may lack the necessary victim support, such as psychological counselling or assistance with evidence collection, which can make navigating the legal process quite daunting.

**Slow Legal Processes:** Cybercrime cases can prolong indefinitely due to procedural delays and the intricacies of evidence collection. This situation often deters victims from pursuing justice.[6]

**5. Enforcement and implementation Deficiencies:**

**Undertrained Law Enforcement:** Numerous law enforcement agencies face a shortage of specialized training in cybercrime, particularly regarding gender-sensitive matters. Officers might lack familiarity with digital evidence or might not consider cybercrimes against women seriously.

**Insufficient Resources and Infrastructure:** Resources allocated to combat cybercrime, such as forensic technology and cybersecurity teams, may be insufficient, limiting the scope and speed of investigations. Relying too heavily on tech companies can be a concern since laws typically mandate that social media platforms remove offensive content. However, the effectiveness of these measures relies on the companies' individual policies, which may be lacking in transparency or vary significantly.

## VIII. THE NEED FOR REFORM IN CYBERCRIME LAWS IN INDIA

India encounters numerous challenges in its legal and enforcement frameworks when it comes to effectively tackling such crimes, making reformation imperative. Let's delve into the necessity for cybersecurity law reform in India, with a particular emphasis on safeguarding women:

**1. Insufficient and obsolete legislation:**

**Absence of precise regulations for specific offenses:** The Information Technology Act, 2000 (IT Act) fails to effectively cover contemporary cybercrimes that unfairly affect women, like unauthorized sharing of private images, cyberstalking, and doxing. Existing provisions have limited scope, as the IT Act deals with certain types of online harassment. However, offenses that are specifically aimed at women, such as image-based abuse and deepfake pornography,

[6]Cybercrime and the victimization of women: Laws, Rights and Regulations, *available at;* https://www.researchgate.net/publication/278015875 ( last visited on November 11,2024).

are either not encompassed or lack precise legal language for effective prosecution. Two brr tags added for line breaks. Gender-Specific Protections are essential due to the existing laws lacking specificity regarding gender. This can result in a restricted understanding of how certain cybercrimes specifically impact women, leaving them exposed.

**2. Jurisdictional Challenges:**

**Cross-Border Nature of Cybercrime:** Offenders frequently conduct their activities across state or international borders, leading to intricate jurisdictional dilemmas. When dealing with cybercrimes that are initiated from outside of India, law enforcement agencies encounter difficulties in collecting evidence and bringing foreign offenders to justice.

**3. Inadequate enforcement mechanism:**

**Insufficient Resources in Law Enforcement:** Within India, police and investigative agencies frequently face challenges due to limited resources and insufficient specialized training to effectively address intricate cybercrimes. Exploring digital evidence, especially in incidents of cyber harassment or stalking, demands a set of skills that numerous officers may not have received training for.[7]

**Insufficient Awareness and Sensitization:** Many law enforcement officers are not adequately trained to grasp the implications of cybercrimes on women and may not handle complaints with the necessary sensitivity. This may discourage women from coming forward to report such crimes. Law enforcement frequently relies heavily on social media platforms, expecting social media companies to remove offensive content. Tech companies might postpone taking action because of the absence of clear legal guidelines and limited cooperation with Indian authorities.

**4. Barriers to reporting and limited support for Victims:**

**Societal Stigma and Victim-Blaming:** Numerous women hesitate to report cybercrimes as they fear societal judgment and victim-blaming, particularly in cases involving intimate images. Laws and enforcement systems need to be improved in order to effectively address these social challenges. This would help in creating a secure environment where women can feel comfortable and safe reporting crimes. Insufficient support for victims can be a reoccurring issue. Victims of cybercrimes often need access to psychological counselling, legal aid, and advice on preserving digital evidence. Support services for cybercrime victims, especially women, are scarce in India.

**5. Enhanced cyber awareness and public is crucial:**

[7]Cyber laws of India, *available at*: https://infosecawareness.in (last visited on November 12, 2024).

 [ISSN 2581-5369]

Many women lack awareness of their cyber rights and legal options, often unsure of existing laws or how to report cybercrimes. Nationwide awareness campaigns are necessary, aiming to educate women on their legal protections against cyber abuse.

Digital literacy, particularly among rural and disadvantaged women, continues to be inadequate. Reforms should incorporate educational initiatives to encourage safe online practices and enhance awareness of potential cyber threats.[8]

## IX. SUGGESTIONS AND STEPS HOW TO TACKLE THE CYBERCRIME

**Change passwords from time to time**: In fact, we all love to easily remember passwords because it is easier. If you want to reduce the risk of online crime, changing your password is a great way to make personal information and social networks safe and difficult for cybercriminals to access (Pennelli 2012). A confusing or complex password protects all accounts, including cell phones, email, landlines, bank accounts, credit cards, etc., and is difficult to guess. Even secret questions should not be answered easily (Moore, 2009). The most secure passwords contain letters, numbers and symbols. Avoid dictionary words and important dates that require different passwords for different websites (Online Privacy and Security Tips 2010). But changing your password can be very helpful in protecting your privacy.

**Avoid revealing home address**: This rule applies especially to women who are business professionals and are highly visible. They can use a work address or rent a private mailbox. Thus, it can help them avoid cyber stalkers (Moore 2009). In addition, women should avoid uploading a large amount of their information to the Internet so that no one can easily access it.

**Maintain stable social relationship**: There's also the fact that we all want to believe we should have 2,000 friends. Dunban's number refers to the limit of the number of people with whom a person can form decent social relationships, and that number is 150. We probably don't need those 2,000 Facebook friends because we probably won't know more physically. more than 150 of them limiting the number of people ensures that our information is shared with people you really know and away from friends of friends you don't know very well (Pennelli, 2012). Women should stay away from unauthorized friendships.

**Cybercrime Awareness Campaign**: Awareness campaign should be created at grass root level like schools, collages etc. on cybercrimes such as stalking scams, financial scams, defamation, misuse of e-mail websites and social networks, virtual rape, cyberpornography, e-mail scams,

[8]India's cybercrime problem and the need for legal system reform, *available at*; https://www.researchgate.net, (last visited on November 15, 2024).

etc. (Halder and Jaishankar 2010: 22). These campaigns can be fruitful in harming cybercrimes.

**Seminars and workshops to better understand cyber-victimization**: Police, lawyers, social workers and NGOs should be invited to educational institutions, clubs, corporate offices, awareness campaigns, seminars and workshops to discuss the legality and illegality of cyber-behaviour adults, including both sexes. Direct reporting of cybercrime victims to the police and NGOs at all levels should be encouraged. Second, workshops and seminars must be organized for police officers to better understand this type of victimization and respond quickly to complaints. Academic and legal experts, non-governmental organizations, etc. should be invited to such workshops and seminars (Halder and Jaishankar 2010: 22).

## X. CONCLUSION

Crime against women in India is not a recent phenomenon. Cybercrime, in particular, has introduced a new dimension to this issue. In the 21st century, a new digital world has emerged, where the internet plays a vital role in every individual's life. Cybercrime poses a significant threat, impacting the safety, dignity of women, and the broader society. It infringes upon the privacy rights of women. The longer women spend online without being aware of the dangers of the Internet, the more susceptible they are. The repercussions of cybercrimes can be highly perilous in all of its various forms, such as cyber stalking, harassment, defamation, and more. The rise in cybercrimes targeting women is causing significant worry among the judiciary, government, and society at large. The repercussions of cybercrime can be extremely menacing and pose a significant threat to both the mental and physical well-being of the victims. It brings considerable suffering to women, sometimes leading to tragic consequences like suicide if not promptly addressed. Cyberbullying can have numerous psychological repercussions on the victim, and the healing process may take time. It is the shattering of his pride, sense of security, and a blow to his dreams and aspirations for the future. In many instances, cybercrime stems from a lack of awareness, vigilance, and knowledge regarding safe Internet usage. Most often, women are hesitant to take legal action against the perpetrator due to concerns related to family reputation, societal expectations, or mistreatment by law enforcement. This is a field that requires the dedicated attention and effort of the research team. Appropriate counselling from specialists, along with emotional support from family members, assists the victim in overcoming pain and anxiety. The Indian constitution encompasses various provisions dedicated to the welfare and safeguarding of women.

Some special provisions were included where necessary to safeguard the rights of women. The government has established a cybercrime reporting platform to combat cybercrimes targeting

 [ISSN 2581-5369]

women and children (CCPWC). The state's smart police force has been assigned the responsibility of monitoring cybersex workers by tracing their IP addresses. They focus on identifying those who exploit the internet to commit cybercrimes against women and children. Women in India have limited access to justice.

Illiteracy, social, and cultural barriers, lack of support from family and subordinates - these are the factors contributing to the difficulties. The legal process, which is both time-consuming and unhealthy, also plays a role. This is also the primary reason why many cybercrimes go unrecognized and unlogged. An in-depth examination of every aspect is necessary to address the issue of cybercrime against women. Make sure to consider all relevant factors. Strict legal action should be taken against the offender. One of the primary responsibilities of women is to educate themselves about various social issues and find the courage to speak out against injustices. Many innovative software is available that can detect various forms of cyber stalking, including tracking of email IDs. It can be suggested that combating cybercrime against women as part of Indian Penal Code reforms necessitates governmental initiatives, alongside shifts in mindset and awareness within the Indian education system and society.

*****

 [ISSN 2581-5369]