

Protection and Empowerment of Women in the Era of Cyberspace: A Strategic Imperative for India

Sameera Khan*

Abstract

The advent of the internet turned over a new leaf for mankind as it turned the world into a Global Village and enhanced communication across the globe. It also plays an important role in the empowerment of women as they can access knowledge, information, and services, which was a distant dream for them. They now have the ability to learn new skills and engage in multifarious activities that were narrowed down due to the archaic era which defined traditional gender roles for women. It also provides them with a platform to voice their opinions, interact with the outside world and raise their voices on gendered social issues. However, it is crucial to understand that women have been the victims of violent and heinous crimes for ages. They are often considered as scapegoats and targeted for the commission of socio-legal damages, wrongdoings and crimes transpiring in the Indian society. The cyber space has been no dissimilar for women as they are exposed to crimes like cyber defamation, sexual harassment, indecent exposure by men on the internet, email misrepresentation and much more. They are vulnerable to receiving sexual content and inappropriate messages over the internet which amounts to online abuse. As a result, the cyberspace is not able to have the desired positive impact on women. This study undertakes an analysis of the issues faced by women in the cyberspace. It dwells upon the need for cyber security and effective tackling of cybercrimes for protecting women in cyberspace. It offers suggestions to ensure women empowerment in the truest sense.

Keywords: Cybercrime, cyber space, women empowerment, online harassment

INTRODUCTION

“Anyone can fall victim to cybercrime and any computing device can be infected with malware. Nobody is immune to cybercrime”.

—Amanda-Jane Turner

The empowerment of women is a multi-dimensional social process. It consists of components like the self-worth of women, having the right to make choices, authority over their lives and participation in the social and economic order on an equal footing. Feminism emerged as a worldwide movement that sought to empower women and cast off the shackles of subjugation, submission and bigotry. It seeks to lead women to re-access and analyse gender identity with a focus on autonomous distinctiveness. To achieve the above idea, the internet plays an essential and a powerful medium to bring nexus within the feminist jurisprudence to connect women across the globe and unleashing their power through technology.

A strategy which is used to fight cybercrime is the increase of the participation of women in the digital ecosystem. The involvement of qualified, educated and strong-willed women in this particular field would pave way for comprehensive gender-

*Author for Correspondence

Sameera Khan
E-mail: sameera.law@gmail.com

Doctorate of Law from Department of Law, Aligarh Muslim University, Aligarh, Uttar Pradesh, India

Received Date: March 16, 2023

Accepted Date: March 28, 2023

Published Date: April 03, 2023

Citation: Sameera Khan. Protection and Empowerment of women in the era of Cyberspace: A strategic imperative for India. National Journal of Cyber Security Law. 2023; 6(1): 22–31p.

balanced strategies and policies which would cater to the requirements of women and other vulnerable groups in the digital sphere. The stakeholders consulted for formulation of cyber-security policies and programmes on enhancing digital literacy need to focus specifically on the empowerment of women. This should focus on assisting them fight against cybercrimes like cyber-stalking, sextortion, phishing, pornography, cyber-bullying, cyber-trafficking and cyber-hacking.

The internet version of feminism, i.e., the feminism taking place in the cyber space is known as “*Cyber-feminism*”. It is the feminist appropriation of information on the internet and technology. It raises the possibility of female emancipation. It uses cyber space as a place where women can share information, interact and engage in discussions through social forums, take action and engage in activities for their empowerment. It has been stated that in modern times, “*The information galaxy, the cyberspace and the Internet are no longer viewed as a masculine space and tool as women have not only embraced but also used the cyberspace to negotiate and reframe themselves within existing social structure*” [1]. It is a place where women are able to forge networks in their cyberspace and cater to their needs and requirements.

Therefore, it is seen that technology is a dominant mean for connecting women across the globe. Internet has been a revolution and is seen as an equalizer for the genders. However, despite that the access is not shared in a uniform manner. There have been several gender disputes with the right of the usage of internet pertaining to women. Technology is seen as something in the masculine domain. It is one of the major reasons why the number of male users on the internet far outnumber the female users. There is also a gender divide in the creation, designing and production of technology. As a result, males develop better skills and are more adept to utilize the features of technology compared to women.

It is often argued that the balance is skewed in the favour of males since the internet is not a safe space for women. They have to face cyber bullying, cyber teasing and cyber harassment which leads to an unsafe environment for them on the internet. The risk of being a victim of a cyber-crime dissuades them from using the internet. Consequently, it becomes significant to empower women to fight against cybercrime.

Growth of Cyber Crime in India

India is becoming more and more impacted by cybercrime. In 2018, 208,456 cyber-related crimes were reported. More cybercrimes were reported in the first two months of 2022 than there were in the entire year of 2018, at 212,485.

The numbers increased even more dramatically as the pandemic progressed, with reported crime increasing from 394,499 cases in 2019 to 1,158,208 in 2020 and 1,402,809 in 2021. India saw a 15.3% rise in cybercrime between Q1 and Q2 2022. Also, in recent years, there have been a growing number of hacks on Indian websites. Around 17,560 websites were compromised in 2018. A further 26,121 websites were compromised in 2020. In 2021, ransomware attacks affected 78% of Indian organisations, and 80% of those assaults resulted in data encryption. While the average encryption rate was 65%, the average attack percentage was 66% [2].

The data shows a consistent increase in cybercrime since the year 2017 (Figure 1). This shows that the prevalence of cyber criminals on the internet is increasing. This further shows the increasing vulnerability of women on the internet in India since they form a significant portion of the victim of cybercrimes.

As per NCRB Data, “*India registered 52,974 cybercrime cases in 2021, an increase of over 5% from 2020 (50,035 cases) and over 15% from 2019 (44,735 cases). Telangana, Uttar Pradesh, Karnataka, Maharashtra, and Assam account for more than 70% of cybercrime incidents. The average rate of cybercrime incidents (per one lakh population) in the country was recorded at 3.9.*”

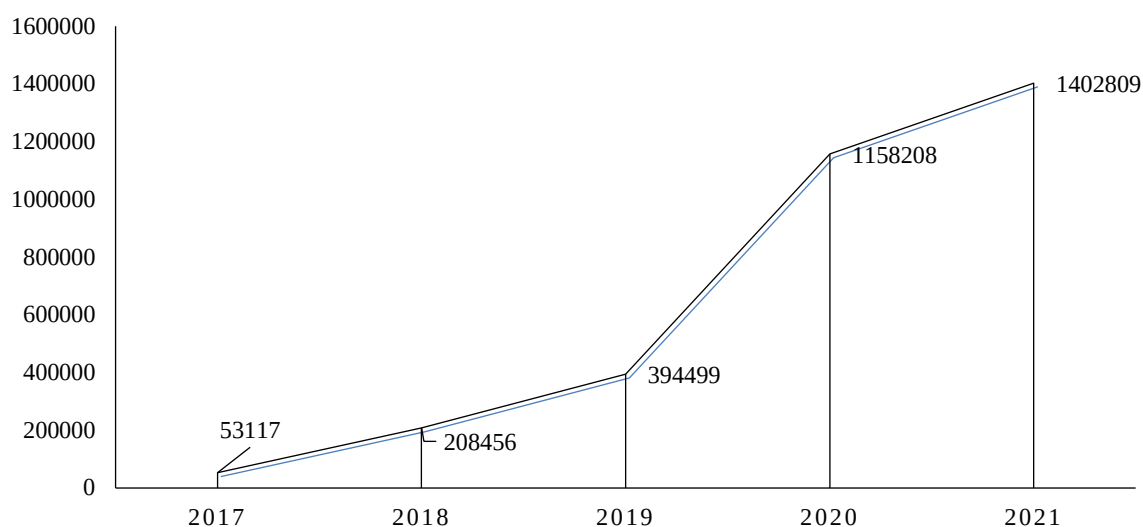


Figure 1. Cyber security incidents in India.

Source: Cert-In.

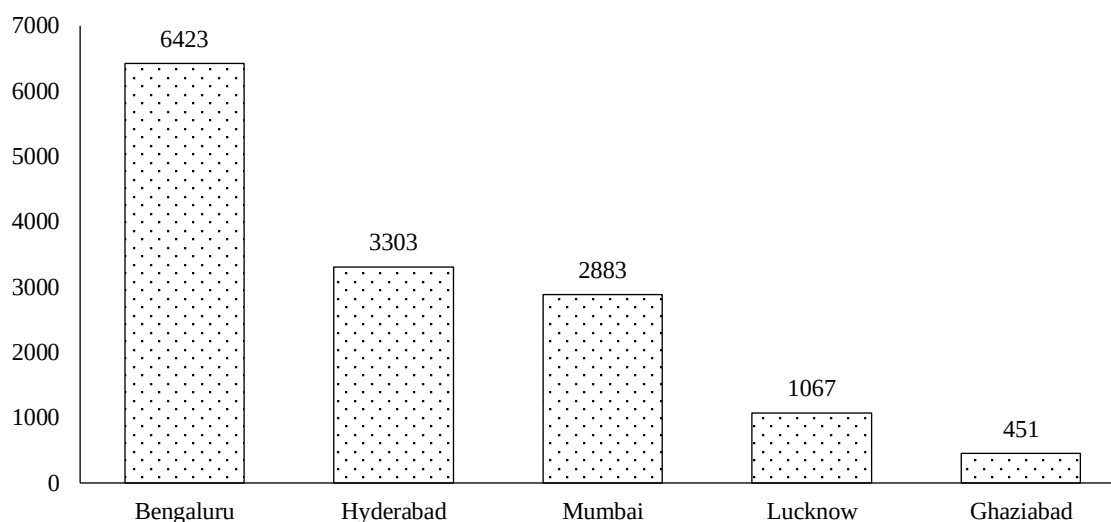


Figure 2. No. of Cyber Crime Cases, 2021.

Source: NCRB.

The Figure 2 shows the cities in India with the highest number of cybercrimes. Bengaluru which is one of the major technological cities in India has the highest rate of cybercrime. These cities are few of the major cities in India and the high prevalence of cybercrime shows that women in these cities are even more vulnerable to cybercrime.

CYBER CRIME AGAINST WOMEN AND ITS IMPACT

Women are most susceptible to Cyber Crime and it can have a grave impact on their life. It was observed by the Union Minister for Women and Child Development, Ms. Maneka Gandhi in May 2016 that, “online abuse of women in India ought to be treated in the same manner as violence against women in the real world.” [3]. This led to the creation of a new forum of redressal and instructions were also provided to the **National Commission for Women** for the creation of a system to take action against the abuse of women over the Internet.

A report was submitted by the **National Commission for Women** after a consultation on cybercrimes in India. The report was titled “*Ways and Means to Safeguard Women from Cyber Crimes*”

in India". In this report, the commission recommended the development of more stringent laws, policies to discourage activities related to hacking, development of dedicated helpline number, imparting of legal knowledge, setting up of cyber forensic labs and imparting special training to members of law enforcement agencies in order to effectively tackle cybercrime.

Impact of Cybercrimes on Women

Cybercrime has a significant impact on women, as they are often targeted for various forms of online harassment, stalking, and identity theft. Women are also more likely to be victims of financial fraud, cyber bullying, revenge porn, and online sexual exploitation. The impact of cybercrime on women can be severe and long-lasting, affecting their mental and emotional well-being, reputation, and even their personal safety.

One of the most common forms of cybercrime that women face is cyber stalking, which involves repeated unwanted online attention or harassment, often with a sexual or threatening nature. Cyber stalkers may use social media, email, or other online platforms to monitor a woman's activities, collect personal information, and intimidate or harass them. Women are also vulnerable to online sexual exploitation, including revenge porn, sextortion, and trafficking. In revenge porn, an intimate photo or video is shared without the woman's consent, often as a form of revenge or blackmail. Sextortion involves the use of threats or coercion to force a woman to perform sexual acts or provide sexual images.

Such cybercrimes have an adverse effect on the overall well-being of women. The psychological and emotional consequences of cyber victimization include, "*depression, suicide, self-harm, anxiety, Post-Traumatic Stress Disorder and fear of future online victimization*" [4]. The consequences of cybercrimes for women can be disastrous and lead to disturbance in future relationships. It can also lead the person to isolate herself from her friends and family. There is also the possibility that the victim feels vengeance towards the perpetrator. It might cause the victim to take some extreme step in the moment of rage in order to fulfil the desire for revenge. This could lead the victim turning herself into a criminal as well. This means that when a woman is a victim of a cybercrime, it can render her helpless, hopeless and have a significant negative impact on her mental and emotional well-being. It functions as a hindrance in the empowerment of the women and has a terrible effect on their progress.

It changes the perception of the internet for women. Such instances are counterproductive to the usage of the internet as a means of empowerment by women. It can cause a feeling of helplessness as they are often victimized in the real world and the virtual world which was an outlet for them to freely express themselves also becomes a place where they feel vulnerable and unsafe. Therefore, it is essential to undertake adequate security measures to ensure that the internet continues to remain a safe space for women.

LEGAL SAFEGUARDS FOR WOMEN IN INDIA AGAINST CYBERCRIMES

It is well-established that women are the most targeted victims of cyber criminals. They often prey on new internet users who are vulnerable to their attacks. As a result, there is a need to provide legal safeguards against cybercrimes to women in order to ensure their safety. The following legislations are present in India with the aim of protecting women from cybercrimes.

Indian Penal Code, 1860

Section 354 A provides for the definition and the punishment for the offence of sexual harassment. It states that, "*A man committing any of the following acts: (i) physical contact and advances involving unwelcome and explicit sexual overtures; or (ii) a demand or request for sexual favours; or (iii) showing pornography against the will of a woman; or (iv) making sexually coloured remarks, shall be guilty of the offence of sexual harassment*".

It further provides that, "*Any man who commits the offence specified in clause (i) or clause (ii) or clause (iii) of sub-section (1) shall be punished with rigorous imprisonment for a term which may extend*

to 3 years, or with fine, or with both". The punishment for a crime contained in clause (iv) is *"imprisonment of either description for a term which may extend to 1 year, or with fine, or with both"*.

Section 354 D provides the definition of stalking. It states that, *"Any man who:*

- Follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
- Monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking".

It further provides the punishment for stalking. It states that, *"Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to 3 years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to 5 years, and shall also be liable to fine"*.

The section has been under the Criminal (Amendment) Act, 2013 and has given stalking a comprehensive definition. Moreover, the legislature also realised that the victims of stalking over the Internet were usually women and the offence as of date can only be made out against a man.

The explanation to Section 354-C of the IPC deals with the instances where the women has given her consent for the pictures to be captured but not for their dissemination. It states that, *"Where the victim consents to the capture of the images or any act, but not to their dissemination to third person and where such image or act is disseminated, such dissemination shall be considered an offence under this section"*. The act also provides for the punishment for the perpetrator. It states that the perpetrator, *"shall be punished on first conviction with imprisonment of either description for a term which shall not be less than 1 year, but which may extend to 3 years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than 3 years, but which may extend to 7 years, and shall also be liable to fine"*.

Section 499 of the IPC provides for the definition of the offence of defamation. A person guilty of the offence can be sentenced to imprisonment for a period of up to 2 years.

Information Technology Act, 2000

There are several instances where the perpetrator befriends the victim and obtains intimate images or videos of the victim. After obtaining these, they are often used as a threat to coerce the victims into sexual acts or distributed online in order to shame the victim. Moreover, they are often used as a tool of revenge by jilted lovers which further creates issues for women. In addition to this, they may even be used for commercial purposes. Section 66 E of the IT Act, 2000 provides for the punishment for such an act.

Section 66E of the IT Act, 2000 provides the *"punishment for violation of privacy"*. It states that, *"Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to 3 years or with fine not exceeding Rs. 2 lakh, or with both"*.

Section 67 of the IT Act, 2000 provides for punishment for *"transmitting obscene material in electronic form"*. It provides that, *"Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to 5 years and with fine"*

which may extend to Rs. 1 lakh and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to 10 years and also with fine which may extend to Rs. 2 lakh”.

Section 67 A of the IT Act, 200 provides for punishment for “publishing or transmitting of material containing sexually explicit act, etc., in electronic form”. It provides that, “Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to 5 years and with fine which may extend to Rs. 10 lakh and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to Rs. 10 lakh”.

Indecent Representation of Women Act, 1986

The Section 4 of the Indecent Representation of Women Act, 1986, “prohibits the production, sale, letting to hire, distribute, or circulation by post any book, pamphlet, paper, slide, film, writing, drawing, painting, photograph, representation, or figure which contains indecent representation of women in any form”. The punishment for the same is provided under Section 5 of the act which states that, “Imprisonment which may extend to 3 years and fine which shall not be less than Rs. 50,000, but which may extend to Rs. 1 lakh”. It further provides for additional punishment in case of a second conviction. The punishment, “may extend to 7 years and fine which shall not be less than Rs. 1 lakh, but which may extend to Rs. 5 lakh”.

This section is useful when dealing with cybercrimes against women since the internet is also a place where the indecent representation of women under the purview of this Section can take place.

Therefore, there are several enactments under the Indian Legislation that can be used to tackle cybercrime against women. They have been interpreted in a positive manner by the Indian Courts in order to provide justice to women. However, their implementation at the ground level is still inadequate which has rendered them unsuccessful in the reduction of cybercrime against women.

Role of National Commission of Women

The “National Commission for Women” (NCW) in India was established under the National Commission for Women Act, 1990. The primary role of the NCW is to safeguard the rights and interests of women in the country and to ensure their empowerment.

When it comes to cybercrime, the NCW plays an important role in raising awareness about the issue and providing support to victims. The commission has set up a dedicated cell for cybercrime, which deals with complaints related to online harassment, stalking, and other forms of cybercrime against women.

The NCW has also been actively involved in creating awareness among women about the safe use of technology and the internet. The commission conducts workshops, seminars, and training sessions to educate women about the various forms of cybercrime and how to protect themselves from such crimes.

Additionally, the NCW works closely with law enforcement agencies and other government bodies to ensure that appropriate action is taken against those who perpetrate cybercrime against women. The commission also recommends changes to laws and policies related to cybercrime to better protect the interests of women.

It launched the Digital Shakti Program in 2018. Its aim was to train women to fight cybercrime. Through this project, over 3 lakh women across India have been educated on cyber security tips and tricks, reporting and redress mechanisms, data protection and use of technology. It has set up an online

resource centre under the **“We Think Digital”** program to help women in trouble with online safety issues like cyberbullying, cyberstalking, financial fraud, etc.

The commission has started a practice where complaints are processed both in person and online. The Commission has launched a pilot project **“Mahila Jan Sunwai”** in partnership with the District Law Enforcement Officers and State/District Police Officers for the facilitation of efficient and speedy redressal of grievances. Moreover, the NCW also takes matters like print, electronic and other media into account. This is done under Section 10(1)(f) of the *“National Commission for Women Act, 1990”*.

In the event that the commission gets a report of cybercrime against a woman, the matter is immediately forwarded to the relevant agencies, including the MHA police's cyber cell, for the necessary response. With the creation of a creative or film on cybercrime security and the dissemination of information via social media channels, the commission has started an awareness campaign.

Role of NCRB

The National Crime Records Bureau (NCRB) in India is the apex national agency for collecting, analysing, and disseminating crime-related data in the country. Its primary role is to support law enforcement agencies in their efforts to prevent and investigate crime. When it comes to countering cybercrime, the NCRB plays an important role in collecting and analysing data related to cybercrime in India. It maintains a National Cyber Crime Reporting Portal, which provides a platform for citizens to report cybercrime incidents online.

The NCRB also collaborates with other law enforcement agencies, such as the Cybercrime Cell and the Central Bureau of Investigation (CBI), to investigate and prosecute cybercrime cases. It provides training and capacity-building programs to law enforcement agencies and other stakeholders to improve their skills and knowledge in dealing with cybercrime. Furthermore, the NCRB works closely with international organizations, like the Interpol and the **“United Nations Office on Drugs and Crime” (UNODC)**, for exchanging information and best practices related to cybercrime.

JUDICIAL APPROACH TO TACKLE CYBER CRIME AGAINST WOMEN

The Indian Judiciary has a major role to play in safeguarding the Indian women from cybercrimes. There have been numerous instances where the Indian Courts have dealt with cases pertaining to cybercrimes. They have acknowledged that the cases have had a significant negative impact on women and have taken a broader stance in most cases to accommodate the new found instances of cybercrime. It has further been done as a deterrent to prevent the occurrences of similar incidents in the future.

Yogesh Prabhu v. State of Maharashtra [5]

The defendant had been accused of cyber stalking by the complainant. An investigation was conducted into the incident and a clear case of cyber stalking had been established. This led to the conviction of the petitioner under Section 509 of the **“Indian Penal Code, 1860”** and Section 66 E of the **“Information Technology Act, 2000”**. It was the first case when an accused had been convicted for the offence of cyber stalking. It also influenced the amendment to the Section 354 of the **“Indian Penal Code, 1860”** where the offence of stalking was specifically added and its definition was enlarged to include the offence of cyber stalking.

Suhas Katti v. State of Tamil Nadu [6]

The complainant stated that the accused had been sending her obscene, defamatory and annoying messages on a message group on the Yahoo website. Moreover, she also received emails from the accused which were forwarded by him using a fake account. Moreover, the victim was also receiving calls from people who were under the impression that she was a sex worker. The police located the accused after investigation and arrested him. He was found guilty of offences and convicted under Section 469 and Section 509 of the **“Indian Penal Code, 1860”** and Section 67 of the IT Act, 2000.

This was the first case where the accused was convicted for the offence of posting obscene messages over the internet.

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra [7]

The employee had been sending out “*derogatory, defamatory and obscene*” e-mails about the Managing Director of the company. The e-mails were sent anonymously. They were sent often to several business associates in order to tarnish the image and goodwill of the company. The defendant was identified by the plaintiff by availing the services of a private computer expert. An ad-interim injunction was granted by the Delhi High Court which, “*restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs*”.

State of West Bengal v. Animesh Boxi [8]

An intimate relationship had existed between the accused and the victim in the instant case. The accused used the promise of marriage in order to obtain intimate photos and videos of the victim. These photos and videos were later uploaded to a porn site without the victim’s consent. A case was filed by the victim before the Court. The court after understanding the details of the case, found the accused to be guilty and sentenced him to 5 years of imprisonment and fine of Rs. 9,000/-.

Avinash Bajaj v. State (NCT) of Delhi [9]

In this case, the director of an online marketing website, *Bazee.com*, came under the scanner. A pornographic video was listed for sale on the website which was taken down within 2 days. However, in the meantime, there had been a few purchases of the video for which the website received a commission. The safety filters of the company failed to detect the video initially and a case was filed against the Managing Director. The court while dealing with the case came to the conclusion that the video was ‘obscene’. Moreover, the company can be said to have committed an offence under Section 292 of the IPC, 1860 due to the listing of obscene material for sale on its website. However, there was no question of the liability of the Managing Director of the company, since the concept of vicarious liability is not a part of the IPC, 1860. There was room to prosecute the director under Section 85 of the IT Act, 2000 if a suit had been filed for the same. The court also highlighted the need for appropriate regulatory framework in order to effectively deal with such cases in the future.

Therefore, the courts also understood the impact of cybercrimes, particularly those against women and have given well-reasoned decisions to support the laws meant for the protection of women against cybercrime. The judicial decisions have come a long way since the Information Technology Act, 2000 in order to ensure that the laws are implemented in a proper manner. This can be evidenced by the fact that the court included cell phone in the definition of a computer system as defined under the IT Act, 2000 in the case of *Syed Asifuddin v. State of Andhra Pradesh* [10]. Therefore, it can be seen that the Courts have played their roles in upholding and implementation of the law. The duty of implementation is with the legislature, the executive and the law enforcement agencies who have to ensure that they perform their roles as per the demands.

CONCLUSION: THE WAY FORWARD

The internet ushered a revolution in human life and changed the world in a way that has never been seen before. It provided a new platform for the empowerment of women across the world. They are now able to network, discuss issues and advocate for causes. It provides them with the opportunity to learn new skills remotely and enjoy access to learning and professional opportunities they did not have before. It gives them a chance to progress in a society even where gender imbalance exists, and their rights are curtailed.

The internet is meant for all people irrespective of gender, caste, class or nationality. Women deserve to be equal beneficiaries of the benefits delivered by the technology, and the products and processes, which materialise from their use. They use the internet for education opportunities, healthcare

information, matrimonial information, entertainment, searching for remedies against injustice suffer and talking to other women to discuss their issues and address them in an effective manner. Cyber feminism is concerned with how new technologies affect women's lives and how subtly gendered cyber culture is in everyday life. In order to combat racial and gender privilege, feminists use the internet as a vital tool for linking women throughout the globe.

A country that wants to flourish and prosper cannot afford to ignore women's empowerment and capacity building. The same information that is available to men and women via the Internet and cyberspace is also accessible to women. Women must be included in all stages of the technology development lifecycle since they are both agents of change and beneficiaries. Cultural and socioeconomic restrictions, which are extremely complicated and also severely impact women. This leads to widening of gender gap over the internet. Without the focused involvement of policymakers and other stakeholders, it is unlikely that the gender gap in Internet usage will narrow on its own. Cybercrime further adds to the growing difficulties of viewing the cyberspace as a safe space for women to empower and flourish.

The legislature has taken note of the growing crime against women and has amended the laws accordingly to accommodate for more provisions that specifically deal with crime against women. Moreover, the IT Act, 2000 and the IPC, 1860 have been regularly amended in order to keep pace with the changing times. The courts have also taken a progressive viewpoint and ensured that online perpetrators do not go unpunished. Despite the measures taken and the enactment of laws, implementation remains a key concern. In addition to this, there is a general lack of awareness amongst first-time internet users about the potential dangers of the internet. Moreover, the victims are often clueless as to how to report the crime and the situation tends to overwhelm them. In addition to this, in cases where the crime is accompanied by threats, it can become even more difficult to report it. Therefore, the State must take measures to remedy the situation and ensure that the internet is a safe space for women, and they do not fall victims to cybercrime.

The menace of cybercrime is limited not only to India but is a global phenomenon. Therefore, the efforts of one state cannot be sufficient. There is a need for global cooperation on the issue so that it can be tackled more effectively. In addition to this, the mechanisms for the redressal of grievances should be made more accessible. The public must be informed about ways to register grievances. The major objectives should be to enhance the ease of lodging of complaints and reducing the delay in prosecution and investigation.

In order to ensure that the cyber space remains a safe space for women and acts as tool for their empowerment, the following suggestions can be implemented:

- An efficient portal specifically dealing with cases involving cybercrime against women must be developed. It should be easy to access for women and the response time should be quick to ensure it is able to serve its purpose. The current infrastructure needs to be upgraded to build more trust in the system.
- The women on the internet are often not aware of the rights and remedies available to them. To make them aware, regular awareness sessions should be conducted all over the country by the Government in collaboration with NGOs and other organizations. They should be used to educate women regarding the safe way of using the internet and identifying cyber criminals so that they can stay safe. They should further be made aware of the process of filing a complaint if they are a victim of cybercrime.
- The usage of cyber security technology amongst women users should be promoted. They should be encouraged to use strong passwords and not share with anyone including trusted friends and family members.
- The social networking sites also have the obligation to create a safe space for all the users on the internet. They are places where users divulge their personal information which may be misused

if the security framework of the social media site is not robust. Moreover, they need to develop a grievance redressal mechanism and cooperate with law enforcement authorities when dealing with cybercrime. They must provide the information required to track the offender to the authorities.

- The internet is a place where the content spreads like wildfire and the more the delay, the more the damage is caused to the victim. Therefore, it is essential that the steps related to investigation and prosecution are carried out expediently. The justice delivery mechanism should be efficient.
- The victims of cybercrime often face serious mental health issues which may cause them to take irrational decisions that can lead to self-harm. The provision of counselling services for the victims of cybercrime will help them deal with the situation better and deal with the adverse effects of the incident.
- The cybercrimes are often not limited to only one country. The perpetrator may be in a location outside India, which means that the power to prosecute him with the Indian agencies is negligible.
- The Government should undertake initiatives for empowering women digitally. They should start skill development programs and digital vocational training programs to assist in the development of digital skillset.
- The government should strengthen laws related to cybercrime against women, making them more comprehensive and stringent. Laws should be updated regularly to keep up with new forms of cybercrime. The framework should aim to empower women and promote the internet as a safe space.

The fight against cybercrime against women requires a comprehensive and coordinated approach involving various stakeholders, including the government, law enforcement, civil society, and private sector organizations.

REFERENCES

1. Eng Kuah-Pearce K. Chinese Women and the Cyberspace. Amsterdam: Amsterdam University Press; 2008.
2. Aag It. (2023). The Latest 2023 Cyber Crime Statistics. [Online]. <https://aag-it.com/the-latest-cyber-crime-statistics/>.
3. Deccan Chronicle correspondent. (2016 May 18). Online trolling against Women to be considered violence: Maneka Gandhi. [Online]. Deccan Chronicle.
4. Brown CF, Demaray MK, Secord SM. Cyber victimization in middle school and relations to social emotional outcomes. *Comput Hum Behav.* 2014; 35: 12–21.
5. Yogesh Prabhu v. State of Maharashtra, C.C. No. 3700686/PS/2009.
6. Suhas Katti v. State of Tamil Nadu, C No. 4680 of 2004.
7. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, CC No. 4680 of 2014.
8. State of West Bengal v. Animesh Boxi, C.R.M. No. 11806 of 2017.
9. Avinash Bajaj v. State (NCT) of Delhi, (2008) 150 DLT 769.
10. Syed Asifuddin v State of Andhra Pradesh, 2006 (1) ALD (Cri) 96.