Chapter 6

CONCLUSION & SUGGESTIONS

The Information and Communication Technology has witness unparallel and extraordinary growth. The expansion of the Internet has been phenomenal, from a sheer convenience platform to an all-pervading concept on which our everyday life is sustaining. The reach of the Internet is such that it has surrounded us to the extent that we have become oblivious to its importance in our lives. The Internet has brought a revolution in the dissemination of knowledge, exchange of ideas and cultural values and in creation of diverse opportunities. The Internet is a marvel worth appreciating and commending. However, while lauding the benefits of the Internet, we should also keep in mind the dangers entrenched in its use. Cyberspace has become an easy apparatus for offenders to victimize and violate women. Indisputably modern innovations have been a boon to women like men, as ICTs have immensely helped in removing the social and economic barriers faced by women. The Internet has simplified the lives of millions of women across the world, but simultaneously, these technologies have also led to a blatant increase in the crimes of online violence against women. With the progress of technology at a fast pace, crimes like cyber crimes have increased drastically and day by day, the menace of cyber crimes is increasingly targeting vulnerable groups like women and children.

The Information and Technology Act, 2000 was enacted in India to fill the vacuum in the area of cyber regulation. The object of the IT Act, as highlighted in its preamble, indicates that the act was enacted primarily to enhance e-commerce. Hence, it categorically covers crimes of commercial or financial nature such as hacking, fraud and breach of confidentiality etc. However, at the time of the enactment of IT Act, the

lawmakers were not acquainted with the risks that the misuse of technology can pose to privacy and reputation of the users. Cyber crimes are easy to commit with little resources and the consequences can be devastating to the safety and security of women.

Violence against women is not a new phenomenon. It is a severe infringement of human rights and has existed since long. Violence against women has continuously changed shapes and forms from time to time in Indian society. With time, many feminists have raised their voices condemning all forms of violence against women and raising support for ameliorating the position of women in society. Even though after independence, much has been done towards the empowerment of women, yet there is no end of her miseries as women still are vulnerable and are an easier target for exploitation. The emergence of Information technology brought a grand revolution in the communication space. Today the world has come closer and ICTs development has made the world a 'Global Village'. ICTs have also greatly benefitted women by giving them equal space for the realization of rights. The invention of the World Wide Web along with the development of mobile phones and other ICT enabled gadgets have greatly improved standard of life of all, including women. Although these technological inventions offer enormous benefits for all, it also has harmful effects on our life, if not properly and adequately regulated.

The Information Technology Act, 2000 has many provisions dealing with various forms of cyber crime yet the Act is silent on issues of harassment faced by women on the internet and does not specifically cover any cyber crimes against Women. The IT Act fails to keep into consideration gender vulnerability and the adverse effect of the crime on women victims. Under the mandate of Article 15 (3) of the Indian Constitution, women-centric provisions and special protections are to be enacted by

the state. The primary reasons for such an inclusion in the Indian Constitution are the recognition of the vulnerability of women and the need for special protection. By analysing the IT Act, it is observed that other than S.72, no specific mention of any protection to women is sought to be accomplished by the IT Act, 2000. The introduction of women-centric cyber laws prescribing deterrent punishments, shall serve a stern warning to the troublemakers, which shall aid in curbing of majority of the online offences against women.

Everyday many women face sex-related harassment, discrimination and online violence in the cyberspace only because of their gender. Many women bloggers, online artists, professionals and social media users with or without, prominent profiles regularly face the threats of rape, violent pornographic material, sexual harassment, accusations of promiscuity and various other forms of humiliation on a daily basis. The issue of cyber victimization of women is not a problem that is limited to India or some developing countries. Today the issue has become a global concern. However, unfortunately very little conversation or legal recourse has developed around the issue.

In past, women victims who had to face abuse and harassment online did sought some legal relief and recourse through Section 66A of the IT Act, which now stands repealed by the Supreme Court judgment in Shreya Singhal v. Union of India[1]. Alarmed at the frequent, use of the provisions under Sec. 66A to make arrests, a Public Interest Litigation was filed before the apex Court questioning the constitutional validity of Section 66A of IT Act. The Hon'ble Supreme Court declared that Section 66A was violative of Articles 14, 19 and 21 of the Indian Constitution

[1] 223 2013 12 SCC 73

that guarantee the fundamental rights to equality, free speech and life respectively and it could not be accommodated in any of the exceptions listed in Article 19(2) of the Constitution. The Hon'ble Supreme Court while striking down the provision of S.66A expressly recognized the vagueness and over-breadth of the provision leading to misuse. The Court emphasised on the issue with vague formulations of domestic laws and stated that it prevents individuals from understanding what is and what is not prohibited. This confusion created by the vague formulation of law opens up the possibility of misuse of the provision by the police. The Hon'ble Supreme Court also observed that clearly the use of expressions in section 66A of the IT Act, 2000 are undefined, vague and completely open-ended. The expression covers within its ambit, a protected speech that is innocent in nature and is liable therefore to be used in such a way that it can have a terrifying effect on free speech. Section 66A was thus struck down because of the damaging effect it caused on a fundamental aspect of democracy.

The deletion served as a boon for the right to free speech and expression but at the same time, it has struck a significant blow on the rights of female internet users. Section 66A of the IT Act, 2000 did suffer from vagueness and ambiguity in terminology and the interpretation of the provision was open to be abused and misused by the government agencies. However, the IT Act, 2000 was created with the objective of providing adequate protection against various forms of cyber crimes prevalent in the society and the enactment of the penal provision contained in the IT Act were never intended to restrain or curtail the right of free speech and expression. The court while interpreting the provision of section 66A of the IT Act, should have taken into consideration the overall scheme of the Act along with the aim and object of the Act. Another point favouring S.66A was that it was the only provision under the IT Act that was used to provide for adequate protection for the female internet

user community as a whole. The said provision being broader in content included within its ambit any kind of internet based harassment that could have been committed in the cyberspace, to bring to book a wrongdoer. Unfortunately, section 66 A was scrapped, and despite some use of the section to counter cyber victimization of women, the said provision of law could not find a place.

In various instances of cyber victimization of women, especially through the offences like morphing of image for circulation or the creation of a fake online profile to provide indecent description of a woman victim, a profoundly negative impact is left on the victim. The issue is further aggravated by the fact that the indecent representation remain 'alive' on the internet for a long time period and goes on to create more embarrassment for the victim, with every passing day. Such cyber victimization tarnishes the personal as well as professional reputation and well-being of the victim. In most instances of cyber violence, a fake profile is knowingly left open for public viewing for causing more harm to the victim. Also the content once removed can again find its way to the internet and the same is uploaded and updated multiple times in search engines easily by the perpetrator. The virtual world offences have far-reaching and devastating consequences upon the victim as it ruins the physical health, mental peace, can also lead to financial loss and loss of reputation and in extreme cases can lead to physical harm also. The IT Act is the primary law for the regulation of the cyber world, but unfortunately the Act is a half hearted attempt to resolve serious issues of victimization especially towards women. While India remains one of the first few countries to enact the IT Act to curb and control the issue of cyber crimes, yet it is unfortunate that the issues regarding online violence of women remain untouched and ignored under the Act. The IT Act has provided for certain specific offences such as hacking of a system, publishing of obscene materials

in the net, tampering the data etc., as punishable under the law. However, an important concern regarding the protection of women involving a great threat to the security, privacy and dignity of women, in general, is largely ignored under the IT Act. With time, the exposure to technology has also increasing become a source leading to the increase in the cyber crime rate. The technology use against the vulnerable and weaker section of the society has become a major issue that needs to be redressed.

The Information Technology Act, 2000 extends to the whole of India and the act also applies to any offence or contravention of the provisions that is committed outside the territories of India by any individual, irrespective of the person's nationality. However, in case an offence is committed by any foreign national under the IT Act, 2000 legal assistance and co-operation is necessary from concerned authorities of the country to which the foreign national belongs, as assistance is required for the purpose of the investigation, prosecution or extradition.

This legal assistance is difficult to procure in most of the cases as India is not a signatory to Convention on Cybercrimes. The said Convention is the only international convention that puts emphasis on the prevention and punishment of crime in cyberspace. As per the preamble of the Convention on cyber crime, the objective, of the international agreement is to create a standard criminal policy that aims at the protection and prevention of cyber crimes. The convention envisages the adoption of appropriate state legislation and steps to be taken for fostering of international co-operation to tackle cyber crime cases.

As the cyber crime can be committed with ease, a significant impact is created in cases of cyber crime and because electronic evidence are easily tampered or are

volatile, it becomes imperative for the law enforcement agencies to quickly trace the offender and take cogent steps to preserve the original evidence. Moreover, the tracing of an offender in cybercrime cases becomes extremely difficult owing to the availability of several techniques to camouflage one's identity. For proper investigation and effective prosecution of cyber crime matters, quick action is required as evidence is volatile in nature and if the collection of electronic evidence is not done promptly, the whole process of evidence collection shall stand defeated. Thus, it is important to forge international co-operation and provide mutual assistance to curb and control the menace of cyber victimization as cyber crimes generally are multi-jurisdictional in character.

In 2013, a study was conducted by the United Nations Broadband Commission for Digital development, on the emerging problem of cyber crime to examine the options to strengthen the existing legal regime and to propose national and international legal or non-legal responses to cyber crime. The report concluded that there are a wide range of national legislations dealing with cyber crime and international cooperation. However, there is a dire need for the harmonization of legal frameworks in consonance with the international regime so that there is no confusion or limitation imposed on the law enforcement agencies. The harmonization process should ideally cater to the following areas like definition, meaning and types of cyber crimes, investigative powers of police, and rules relating to the admissibility of electronic evidence before court.

1. Recommendations to meet Legal Challenges

When it comes to cyber crimes against women and its treatment under the India law, the legal set up suffers from various issues which need urgent rectification.

i. The unstructured and incomplete legal protection provided to women against cyber crimes has led to a situation wherein women have lost faith in law enforcement agencies and the judiciary. Instead, to find a quick solution to their problem, they approach hackers to help them either reclaim their account or to remove offensive contents. There is an urgent need for improved policies and stricter laws to discourage hacking activities among the youth and to dissuade victims from approaching hackers for removing offensive contents from the Internet, mobile app etc.

ii. India must enact rigid and stringent laws for addressing the issue of cyber victimization of women. Information Technology Act, 2000 (as amended in 2008) in the present form does not take into considerations the unique needs of women victims. The IT Act is not a women sensitive Act. The present research, along with increasing research on the subject of cyber victimization, has highlighted the need for women-centric laws to combat cyber victimization of women. It is high time that the IT Act should be reviewed to introduce innovative approaches in law. A woman-centric information technology law must be drafted defining types of cyber crime targeting women. There is a need for the enactment of stricter guidelines for intermediaries to pull down content offensive to women. As trans-Jurisdictional issues are involved in most of the cyber crimes, there is a need to develop a trans -jurisdictional mechanism by signing bilateral treaties.

iii. The unstructured development of laws regulating cyber crimes in India often leads to confusions as to the application of the law. It is pertinent that the existing provisions of the Information and Technology Act, 2000 and Indian Penal Code should be reframed into a constructive law. Provisions from

Indecent representation of Women Act, the Indian Telegraph Act, 1885 and other laws must be included in the new law to create a complete code dealing with cyber crimes and cyber regulation. Either the IT Act should be re-modified or a separate law should be enacted to deal with cyber crimes.

iv. Most punishments under the IT Act are bailable. The cyber offences targeting women should be given a serious treatment. To create a deterrent effect in the society, cyber offences against women, should be made non-bailable and cognizable. The punishment term must also be enhanced from simple imprisonment terms for six months or one year, from a minimum of three years to a maximum of five years. Further, the punishment should be of more than seven years or more imprisonment in cases of a grave offence.

v. Anonymity provides a fertile ground for the cyber-criminals to breed and prosper. Cyber-criminals are operating multiple accounts in order to humiliate and abuse women online. There is a need for floating of a scheme to create mandatory Uniform identification number creating accounts in the social media.

vi. "Right to access the net" and "right to be forgotten" policies have gained momentum in the west owing to the recognition of the issues in the cyberspace. Such policies must be incorporated in the Indian laws to provide adequate protection to women and other vulnerable groups. Further, owing to the significant nature of these rights to secure the privacy of an individual, such rights must be conferred the status of fundamental rights under the Indian Constitution.

2. Recommendations to meet Socio-Psychological Challenges

The incidence of crime against women, which are rapidly increasing in new forms and ways, is primarily attributed to the socio-psychological view prevalent in society. The misogynist and patriarchal view are mainly to be blamed for the subjugation and abuse of women. Cyber victimization of women is also brought about by the same prevailing thought. Further, the cyber crimes against women remain mostly unreported due to the hesitation of the victim to approach the law enforcement agencies and her fear of loss of reputation and defamation of the family's name. Many women victims blame themselves for the crime done. The victim-blaming further done by society makes her feel responsible for the crime, instead of reporting the incidents are taking steps for stopping the harassment, women end up moving away from cyberspace. The women are more vulnerable to the menace of cyber crime as the perpetrator benefits from the anonymous nature of the Internet, wherein the perpetrator may persistently threaten and blackmail the victim with different identities and names. The fact that women do not approach the police to complain against cyber-harassment and they prefer to move away from cyberspace is alarming and needs great introspection at the state level. The government needs to work on improvement of awareness levels and should educate the masses about the perils of cyber crime with emphasis to cyber victimization of women and girls and should address the issue at the grass-root level by reaching every citizen of the country and empowering them with cyber hygiene and cyber etiquettes. Thus, a mere legal solution will not be enough to combat the issues of cyber victimization of women. As regards the socio-psychological challenges are concerned, the following steps can be incorporated:

i. Awareness programmes and campaigns should be organized at the grass-root level, such as schools and colleges to enable children and youngsters to learn about the dangerous consequences of misuse of information and Communication technology. Amongst other relevant themes regarding the use of cyber technology focus should be on creating awareness on existing and newly evolving varieties of cyber crimes targeting women like cyber stalking, online defamatory activities, misusing of social networking websites, cyber pornography etc. The awareness programmes should be effective enough to inculcate the understanding of prevention and protection from cybercrimes, socio-legal ethics regarding photography in public places, especially photography of women. Efforts should be made to instill safe user habits in the cyberspace and to make people aware of legal rights and duties towards respecting the right to privacy, right to life and liberty. Knowledge of cyber hygiene and cyber etiquettes should be imparted through these awareness programmes. If properly planned and executed, these campaigns can be valuable and fruitful in paralyzing the growth of cyber crimes.

ii. Awareness camps should also be organized for adults including teachers and parents regarding the duties to monitor children's behavior on the Internet, monitor the use of digital devices by young children, teach children and teenagers about safety norms in the cyberspace and encouraging them to report cyber crimes to parents, teachers and law enforcement machinery.

iii. Government/Organisations must be encouraged to develop favourable policies, especially at the workplace, to help women to come out of the "feeling of shame" and report crimes to proper authorities.

3. Recommendations to meet Technical/Implementation challenges

Wherever societal interaction occurs, criminals are sure to follow. Cyber crimes are the most striking example of this. With advancements in technology, modern society has become more dependent upon computers and the Internet has invaded every part of the world. The computer criminal has, in turn, immensely benefited from the development of technology and has used the ICTs to his advantage. Cyber crimes are being committed with more sophistication. Cybercriminals are clever and use sophisticated gadgets that are not easy to trace. Also, cyber crimes may be non-local in character as the action can occur in faraway jurisdictions. A person can easily commit a cyber crime while sitting in any country. The investigation agencies do not get adequate cooperation from social media networks and service providers. Further, investigation officers, especially the lower level policemen, are not adequately trained to handle computer hardware and software.

Over two decades since the government has passed the IT Act to address the problem of criminal activities that take place over the Internet, not much respite has been given to Internet users. Cyber crime is growing in new ways and forms while the law enforcement agencies are seen struggling with the issue.

There exist plenty of laws on the books, but enforcing them is often not easy for the law enforcement agencies and the judiciary who are grappling with the issue of lack of technical knowledge and deficiency of adequate technical infrastructural support. It can be immensely frustrating for the victims of cyber crimes to know that the perpetrators are never brought to justice. The police departments have set up divisions and cells devoted explicitly to computer crimes enforcement. However, there is still a lack of proper training and understanding of cyber crime amongst the police force,

especially at the lower levels. For several reasons, enforcing laws governing online behavior is more complicated than the enforcement of 'traditional' laws.

Thus, the cyber world presents an uneven playing field to the law enforcement agencies when compared to the benefits accessed by the perpetrators. With regard to the technical set-up, it is crucial to have updated and sophisticated labs to meet the growing challenges of cyber crime. Without a sound technological set-up, the law enforcement agencies cannot nullify the advantages of anonymity and privacy enjoyed by the cyber-criminals. The technical and implementation challenges cannot be ignored in light of the legal and socio-physiological challenge. Sufficient resources and time are to be allocated by the government on the aspect of technical and implementation barrier. Though a few steps have been taken in this direction, yet some more steps are required to remove the hurdles. The following steps could be taken to solve the technical and implementation challenges

i. Policies should be framed on compulsory training of all the police officers for dealing with cases on information technology. Further, the government should promote workshops and refresher courses for police officers for up-gradation of knowledge in the field of cyber laws. Further, police authorities investigating the cases related to cyber crimes apart from IT Training should also be trained in dealing with women victims keeping in mind the victim's psychological position. Thus there is an urgent need of a mechanism that focuses on giving assistance for psychological up-gradation of women victims.

ii. Policies should also be brought in place for the creation of cyber crime cells in all police stations and for deploying more women officers in cyber cells.

iii. Well equipped cyber forensic labs in each district police headquarters should be set up. Steps should be taken to ensure proactive policing for dealing with cases of cyber crimes against women.

iv. Laws such as Section 292 and 294 IPC restricting illegal and unauthorized selling of digital devices and porn contents and punishing obscene acts and songs should be implemented in letter and spirit.

v. *Mahila Courts* which have been set up to deal with the cases concerning crime against women such as dowry harassment or custody cases for children and is presided by a woman judge may be given the power to deal with cases of cyber crime against women.

vi. Police and policing is not a complete solution. Role of Social Media and self-restraint are also important. Further, proper cooperation between victims, police, judiciary, social media, service providers and various stakeholders is required to deal with cyber crimes.

vii. There is an urgent need to adopt a uniform law dealing with cyber crime at the international level because cyber crime is not a national problem but an international issue which requires the international community to come together and look for feasible solutions. The need to adopt specific legal provisions dealing with the issue of jurisdiction and to develop some basis of international co-operation cannot be over-emphasised. India should become a member of the European Convention on Cybercrime, 2001 and work at the international level to overcome the technical barriers of jurisdiction.

4. Other recommendation

Apart from the above recommendations, certain recommendations which come under the purview of non-legal solutions should also be adopted. These recommendations are focusing on the role of women and social networking sites to make the Internet a safe and secure place. Steps need to be taken from all stakeholders to keep the Internet free from nuisance and violence. It is essential that the Internet users adopt certain non-legal practices. Following are some non-legal recommendations that should be followed:

i. Regular Surveys on Victimization Status:

An essential factor in articulating criminological responses for cyber stalking offences is the availability of reliable information. In India, criminological inferences and strategies are being made based on external data, which reduces the effectiveness of the labours of the criminal justice system. Hence, authentic cyber stalking victimization surveys are necessary to understand the exact nature and extent of the issue at hand. These surveys will help the authorities make better and efficient criminological response for the particular offence.

ii. Self-Regulation

Internet users should be conscious of the fact that there are a number of stalkers online looking out for their next victim. Hence, one should set strong and meaningless passwords that are difficult to crack and also use a gender-neutral username. Active social media users should be cautious of what they post online and should avoid uploading personal / intimate pictures and information.

iii. Regulation of Social Media Sites.

Internet users should give importance to regulations provided on social media sites as it would help them protect themselves from cyber offences. This includes keeping their profiles blocked from being viewed by a stranger. All the existing social media websites give their users various methods of restricting unknown people from viewing their information and photos posted online.

iv. Passwords should be changed from time to time.

People create easy-to-remember passwords for their convenience. However, simple passwords provide easy access to cyber-criminals to invade into the privacy of others and tamper with their online social media accounts. To lower the risk of cyber crime, frequently updating of password is a way to secure the personal data and access to social networks by making it difficult for a cyber-criminal to access. Tricky or complicated passwords protect the accounts from unauthorised access as they are difficult for anyone to guess. Ideally, a secure password should contain a mix of letters, numbers and symbols. Nonetheless, frequently changing password can be helpful to keep personal information private and to secure the privacy of the individual.

v. Avoid sharing personal information: The Internet today is not only used for entertainment but has also become an essential medium for work and business. Information of personal nature like name, telephone number, e-mail, address etc., is thoughtlessly shared over the Internet for work purposes. It is essential that personal information should be only shared with trusted people like friends and family. Working women professionals should not use their private mobile number or e-mail id for work-related communication instead they

should opt for a different mobile number and e-mail for work so that the social networking sites and mobile apps connected with her private number and email are not accessible or visible to others. This step can help women in avoiding cyber stalkers. Moreover, women should avoid uploading personal material on the Internet regarding their private information so that no one can easily view or access them.

vi. Understand privacy settings of social networks: Social networking sites and other service providers are governed by privacy policies and have some or the other options of privacy settings made available to the users. One must try to understand such privacy policies and make use of the privacy settings available. These privacy policies if properly used do help in the protection of personal data thereby protecting a user from any potential risk or online harm.Thus, women must know the privacy settings of social networking sites.

CONCLUSION

The threat to privacy and security of women under the current Indian scenario can be understood and gauged by numerous reported instances of female abuse and exploitation, in the cyberspace. Everyday newspaper reports highlight some form of cyber victimization of women. The concern for growing cyber victimization of women bring into light many important questions with regard to the safety, security, privacy and dignity of Indian women.

Ironically, the cyber victimization of women includes the abuse of fundamental rights guaranteed under the Indian constitution and is a form of gender harassment, in the modern day and age, yet no substantial step has been taken to control and curb this menace. India is one of the first countries to enact a law governing information

technology *viz.* the IT Act, 2000 to combat cybercrimes. According to the preamble of the IT Act, the Act focuses on controlling crimes that are commercial or economic in nature, but there exist no specific provision in the IT Act to protect the security and privacy of women. In the US and UK, there exists various rules and legislation to deal with the issues of cyber victimization of women. While, in India, there exist few general provisions that are often used and invoked to cover some of the online crimes against women under the IT Act,2000. Still, the IT Act depends upon the Indian Penal Code to deal with the crimes in the virtual world.

Crime should be dealt with in nascent stage and should be effectively curbed and controlled, at the first instance, so that they do not develop into grave and serious proportion. Ideally, the Indecent Representation of Women (Prevention) Act, 1986 should be amended to include within its ambit different cases of online defamation and obscenity, since it was created with the specific objective of providing 'aid in addressing the problem of increased objectification of women and thereby ensuring the dignity of woman.' Thus, while the IT Act, 2000 is a gender-neutral legislation, the Indecent Representation of Women (Prevention) Act, 1986 can provide assistance in specifically targeting and eradicating of the notion of cyber crime against women, at the initial stage itself.

The issue of cyber victimization of women cannot be curbed without the help of international treaties and conventions along with the co-operation of other countries. Thus international co-operation is an important aspect that cannot be overlooked since. Cybercrimes being trans-boundary in nature, the prevention of it command the co-operation with other countries with regard to aspect of extradition policy and prosecution rules. Further, the need for speedy disposal of the case cannot be over-emphasised as relevant. The cyber-evidence are intangible in nature and thus

collection of the same shall only be possible if all the states stand together to find a solution to the issue. For fostering an environment of mutual assistance and corporation, the European Union has undertaken many initiatives in the form of European Convention on Cybercrimes, 2001 supported by many international organizations.

Thus, India also needs certain significant changes for reporting and tracing out domestic crimes on the Internet. Further, it is for people to acknowledge that the growing incidence of cyber violence against women is primarily a manifestation of gender discrimination and inequality in gender power relations. Positive steps should be taken at the societal level to remove the gender inequalities and discrimination. Also, India should become a part of the only international convention pertaining to the virtual world is the "Convention on Cybercrimes". This shall go a long way to achieve a uniform standard to deal with the issue at the global level. While the state should do its part to improve laws and collaborate with the service providers to make internet a secure place for everyone. Women should shun the silence and should come forward for combating cybercrimes for securing and protecting their freedom and rights.