PROTECTION OF WOMEN IN CYBER SPACE: IS IT ILLUSIONARY OR REALITY?

Written by ***Mansi Jain Garg* & Subhasmita Subhadarsini Patra*****

** Ph.D. Scholar, Jamia Millia Islamia*

*** 2nd Year BA LLB Student, School of Law, Sharda University*

ABSTRACT

"**This is just the beginning, the beginning of the understanding that cyberspace has no limits, no boundaries**"

-Nicholas Negroponte[1]

The digital era is evident of drastic changes where billions of people across the world have tried bridging the gaps and are multiplying human potential. The credit goes to the world of information technology for bringing humans across the world closer by making it a global village: reliable and easily accessible. It has developed titanic positive potentials, but when these positive potentials are misused it may create havoc. Cyberspace refers to an online world where users have the mechanisms in place to transact any business or personal activity much more easily and freely as they can transact them in the physical world. Just with a single click of the mouse, the cyberspace has given us, the humans, a well-designed e-commerce system which has reduced inefficiencies with a better flow of information. But at the same time, it has resulted in certain social, political, moral implications which have made lives of many miserable. The main victims of cyberspace are women, who get exploited and harassed over social media and due to lack of evidences, or sometimes fear of defamation, and many such other reasons, the culprits are not made accountable for their misdeeds and justice is denied to the victims.

[1] Nicholas Negroponte, Cyber Space Quotes, Brainy Quotes (Nov.10 2017, 3:30 PM), https://www.brainyquote.com/topics/cyberspace

ISSN 2581 3382

The research paper aims to ascertain whether the laws available for the protection of women in cyberspace is for real or is an illusion; whether the laws are sufficient to deal with cases of victimization of women in cyberspace or not and what could be the recommendations and suggestions, if any, to achieve the same.

Keywords: Cyberspace, Digital World, Victimization, Women, Laws, Social Media, etc.

Introduction

As Swami Vivekananda had said "That country and that nation that do not respect women have never become great, nor ever be in future". Women are considered as a weaker sex not only from physical point of view but also from sociological aspect also. The smritis are evident of women being depended on man at every stage of their life. When she is a child she is dependent on her father, when she gets married on her husband, when she gets old on her son. In this land where everyone talks of ethics and values, there a woman is now treated as a commodity and is targeted. With the development of technology there have been massive changes in the cyberspace. At one point, it allows people to connect to the rest of the world. In the other, it has its own cons where a woman is targeted and harassed. Her privacy is intruded and she is led open to the hatred and blame of the society. There are reported cases of cyber stalking, cyber- bullying, posting of obscene materials where 75% of the victims are reportedly woman. So the need of the hour is what those crimes are and whether there are enough laws to protect the victims from the same. If not then what extra measures could be brought to deal with such issues.

Objectives of Study

· To make readers aware about the exact meaning and magnitude of Information Technology Act, 2000.

· To throw light on the existing legal framework regarding protection of women in cyberspace with focus on the Information Technology Act,2000 and provisions under Indian Penal Code,1860 and other International Conventions and Laws.

Learning outcomes and Literature Review:

- Introduction to the legislative provisions regarding protection of women in cyberspace.
- Whether these provisions are enough or not.

ISSN 2581 3382

- Whether these laws are sufficient or any stringent laws are required for the same.
- Whether there should be stringent laws or proper implementation of the current laws or application of both the things to achieve that end.
- Whether these laws are sufficient only over paper or in practice as well.

Cyberspace

Cyberspace refers to the virtual medium of transfer of data globally using the World Wide Web and Internet world. It is the virtual computer world and is an electronic medium used to form a global computer network to facilitate online communication.[2] Cyberspace is the environment in which communication over computer networks occurs.[3] As defined by the Merriam Webster Dictionary, "Cyberspace is the online world of networks and especially the Internet." The definition of the Cyber Security Strategy for Germany, 2011, Germany states that "Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks."[4] At the same time the National Security Presidential Directive 54/Homeland Security Presidential Directive 23, 2008, United States ascertains, "Cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."[5] The definitions of various authorities clearly show that cyberspace is the communication over computer and online transmission of data and information. As per Sec-2(j)[6] of the Information Technology Act, 2000, "computer network" means the inter-connection of one or more computers or computer systems or communication device through—

[2] Cyberspace, *Definition- What does cyberspace mean?*, Technopedia (Dec. 22,2017, 10:40 PM), https://www.techopedia.com/definition/2493/cyberspace.

[3] Cyberspace, *Introduction to Security, Cyberspace, Cybercrime and Cyber security*,International Telecommunications Union (Dec.23,2017,9:30AM),https://www.itu.int/en/ITUD/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf .

[4] Damir Rajnovic, *Cyberspace-What it is?*,Cisco Blog- Security, (Dec.23,2017, 10:15 AM), https://blogs.cisco.com/security/cyberspace-what-is-it.

[5] *Id* at 4.

[6] The Information Technology(Amendment) Act,2008, Act.10 of 2009,Acts of Parliament, 2009 (India).

ISSN 2581 3382

(i)the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii)terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the inter-connection is continuously maintained.

Cyberspace therefore is a wide set-up for the networks to establish proper communication system the online world. Every object has advantages as well as disadvantages and so is applicable to cyberspace. On one hand it allows exchange of data[7] , information and is the domain for any particular record. The interactive flow of information enhances distance and new ways for imparting education. For the students basically it is there teacher which can guide them to prepare for their homework, assignments, quizzes, tests and even it provides them with the virtual laboratory. At the same time it displays information which are unknown to maximum in the world. In short it acts as a hub for the flow and exchange of information as well as data. It even acts as a source of entertainment and makes the lives better and easier.

On the other hand, it has many disadvantages too. It more specifically leads to various cyber torts and cyber-crimes. Cyber torts can been defined as those unlawful acts where computer[8] is used either as a tool or a target or both. It can be used as a tool for the activities like- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking, etc. It can be used as a target in cases like unauthorized access to computer/computer system/computer networks, theft of information contained in the electronic form, e-mail bombing, data hiding, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, trespass to chattels, theft of computer system, physically damaging the computer system. One part shows that it is a civil wrong and the other side of it states it as a crime. Cyber-crimes are any crime that involves a computer and a network for its operation. In some cases, the computer may have been used to commit the crime where as in other cases it may have been the target of the crime. For e.g. The sleeper

[7] Sec-2(1)(o) of Information Technology Act,2000 states 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form(including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

[8] Sec-2(1)(i) of the Information Technology Act,2000 states "computer" means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

ISSN 2581 3382

cells use computer to execute their plans of fear and spread terrorisms. They have used computer as a device to spread terrorism. The computer may also become target of crime. For e.g. Many of the times the terrorists try to hack various websites of the defense and then use that information to achieve that purpose.

Cyberspace is undoubtedly an amazing achievement in the field of technology but at the same time has its side effects too. It not only leads to intrusion of privacy but also leads to commission of crimes especially for women. Privacy has been derived from the Latin word "Privatus" which mean "separate from rest." It is the capability of an individual to keep their information in a secluded manner and reveal them secretively. It is the right of a person or an individual to decide who can access the information, when can he access that information, what type of information can be accesses and how to access that information. The privacy policy has four major dimensions:-

- Privacy of a person.
- Privacy of personal behavior.
- Privacy of personal communication.
- Privacy of personal data.

Article-21 of the Constitution of India states, "No person shall be deprived of his life or personal liberty except according to procedure established by law"[9] It has been interpreted in such a way that it includes right to privacy under the ambit of right to life which further means all those activities and aspects that will make a man's life meaningful, complete and worth living. In **Govind v. State of Madhya Pradesh**[10] , the Court accepted the right to privacy as an emanation from Art. 19(a), (d) and 21, but mentioned it as not an absolute right. The Court assumed it as a fundamental right which is subject to certain reasonable restrictions for the interest of the public.It further mentioned that right to privacy deals with 'persons not places'. In **Naz Foundation Case v. Government of NCT of Delhi**,[11]Delhi HC gave the landmark decision on consensual homosexuality. Right to privacy held to protect a "private space in which man may become and remain himself". It was said individuals need a place of sanctuary where they can be free from societal control- where individuals can drop the mask, desist for a

[9] INDIA CONST. art.21
[10] Govind v. State of Madhya Pradesh, 1994 AIR SC 826(India).
[11] Naz Foundation v. Government of NCT of Delhi 160 Delhi Law Times 277(India).

ISSN 2581 3382

while from projecting on the world their personality which is not their real view. Privacy should include that side of a person to be accepted as the way he wants to be, an appearance that may replicate the ideals of their peers rather than the realities of their nature. In **K.S. Putuswammy v. Union of India(2017)[12],** Right to privacy was regarded as a fundamental right and was said that "Dignity cannot exist without privacy. Both reside within the inalienable values of life, liberty and freedom which the Constitution has recognised. Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and protects for the individual a zone of choice and self-determination".[13]

It is now very clear that right to privacy is 'a right to be let alone'. A person has a right to safeguard the privacy of his own, his family, marital affairs, and procreation, child-bearing and learning among other matters. Any person publishing anything concerning the above matters except with the consent of the person would be liable for such interference to the privacy of the said person.

Article-12 of the Universal Declaration on Human Rights, Article-17 of the International Covenant on Civil and Political Rights and Article-8 of the European Convention of Human Rights have wide ambit on provisions of privacy and have remedy for such interference and attacks. Even after such laws and conventions we can still find that there is intrusion of privacy in cyberspace and especially the women are being victimized. They are followed, harassed via e-mails, threatened of clips being leaked over social media. In India the term "cybercrime against women" includes sexual crimes and sexual abuses on the internet.[14]

What are these crimes over cyberspace?

Hacking: Hacking means unauthorized access to computer system or network and making changes in the content so that the other person may not be able to access it. It is an invasion into the privacy of data and person. It is evident that the hackers hack to demean a woman by changing her whole profile into an obscene and derogatory one. They question on her character and chastity. There are various social networking sites like Facebook, Orkut, Instagram, etc

[12] K.S Putuswammy v. Union of India 2017 (India).
[13] P.169 of the judgement of K.S. Putuswammy v. Union of India.
[14] SOBHNA JEET, *Cyber crimes against women in India: Information Technology Act, 2000,* Elixir Criminal Law 47 (2012) 8891-8895,
(Dec.24,2017, 9:30 PM), http://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf

ISSN 2581 3382

which provide options of privacy policy and maintain private accounts. They also provide an option for reporting the profiles which cause disruptions to the privacy of a person

Cyber Stalking: The word "stalking" means "to pursue or approach healthily". It can be used as something known as online harassment where a person tries to follow a person's movement and actions over the internet It involves invading the privacy by posting messages on the bulletin boards, entering the chat-rooms frequented by the victim, constantly bombarding the victim with messages and emails with obscene language. While Cyber Stalking affects both men and women, women are disproportionately targets, especially of age group of 16-35, who are stalked by men. It is believed that Over 75% of the victims are female. In Cyber Stalking, stalker access the victim's personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim. It simply means hide hunting meaning thereby secretly watching over the actions of another person. It means repeated and unwanted behavior where one person tries to connect with another person and that behavior causes the victim to feel threatened or harassed. For e.g., In Ritu Kholi's case, the stalker posted her residence number and invited persons to chat with her over phone. As a result of which she started receiving calls at odd hours which completely brought a question mark to her married life. She therefore lodged a complaint and the stalker was booked under Sec-509 of IPC for outraging the modesty of a women.

The DU Case is also evident where a law student of DU(Delhi University) created fake profiles of a girl over social networking sites as she denied of his marriage proposal. Further he also posted pictures about the girl being his wife. Therefore, the girl lodged a complaint under Sec-66A of the IT Act and mentioned that she is a victim of cyber stalking and theft of idnentity.

In another case, a 28 year old woman, Neha Ghai was shocked after she received objectionable call, messages and vulgar emails. Therefore she approached the cyber cell and came to know that she is a victim of cyber stalking and was followed over the Internet.

Cyber –Bullying: Today the technology is so advanced that people get connected to each other by just with a single click of the button. But at the same time this click opens them up with thousands of risk. In general, bullying means using superior strengths to influence a person to do a particular act. Therefore cyber bullying is the use of cyberspace as a medium to influence another person to complete a particular activity. It is the use of computer and

ISSN 2581 3382

computer networks and also mobile phones to upset another individual. Cyber bullying is "willful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature."[15]

For.e.g., In a particular incident, a 12 year old girl managed to put her picture as her profile picture and was threatened. A person staying in her neighborhood threatened to misuse her information

Harassment via Emails: Email is a message or a document which is distributed by electronic means from one computer to another. Then how can there be harassment via email. It may include any message or document which contains any threatening appeal. Repeated proposals for love, blackmailing, etc are various types of harassment via emails.

Voyeurism: It means the way of gaining sexual pleasures by watching other persons being naked or when engaged in sexual activity. The Merriam Webster Dictionary defines voyuerism as the practice of obtaining sexual gratification from observing others. Over cyberspace, various videos and photographs are leaked and other persons gain pleasure by watching over them. In one way it is similar to pornography. In pornography the person himself in engaged or is forced to get engaged. But in voyeurism a person's modesty is questioned by taking pictures or making videos when she is naked. The victim have no idea of such things. For e.g., Many women are captured while they change their clothes in the dressing room and those clips are posted over social media which is clear act of voyeurism.

Morphing: Morphing means editing the original picture of a person by another person and then posting the same over cyberspace.When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads them after editing is known as morphing.[16] In social networking sites like Facebook, Orkut, etc when one picture gets posted that is again downloaded and posted by creating some fake profiles which amount to morphing and theft of identity.

Email Spoofing: A spoofed e-mail is something which has its content copied from another mail but has different meaning. E-mail spoofing is the forgery of the original e-mail header

[15] NIDHI AGRAWAL & DR. NEERAJ KAUSHIK, Cyber Crimes against Women, GJRIM Vol.4, No.1, (Dec.25, 2017, 11:20 AM), www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC8yMjE3LnBkZnwvMjIxNy5wZGY=

[16] Id at 15

ISSN 2581 3382

having different content and origin. E-mail spoofing is a term used to describe fraudulent email activity in which the sender's address and other parts of the email header are changed so that the person cannot know that it is originated from an unauthorized source. By changing certain properties of the email, such as its header, from, Return-Path and Reply- To fields etc., hostile users can make spoofed email.

Cyber Defamation: Defamation means publishing something which may cause hatred, ridicule or damage the person's reputation among the right thinking members of the society. Cyber defamation is publishing of derogatory material against another person over the cyberspace which may harm the person's reputation and image. For e.g., A malicious customer review against a company could destroy a small business .A false accusation of adultery could destroy a happy marriage. It takes many years to build something but it takes only 2 seconds to destroy the same.

Cyber Pornography: Pornography means a visual material which contains specific description of sexual organs and sexual activity. Cyber pornography involves posting of obscene materials relating to sexual activity. In involves the use of cyberspace to create, distribute, display pornographic content or obscene materials and to stimulate sexual excitement. For e.g., a Swiss couple in Mumbai gathered some small children and forced them to get engaged in sexual activity. They also uploaded the material over Internet. It was a clear example of cyber defamation where they outraged the modesty of small children.

Reasons of such Crimes.

 Majority of the people do not read the guidelines and terms and conditions of the social networking sites before opening their accounts.

 Some people even share their password with their near and dear ones like their close friends, spouse or their children.

 Most of the people are not aware of the cyber ethics and participate in various feedbacks and other programs inviting spam mails and messages.

 Partial knowledge of the computer and its protection also invites for virus affecting the computer and other software programs.

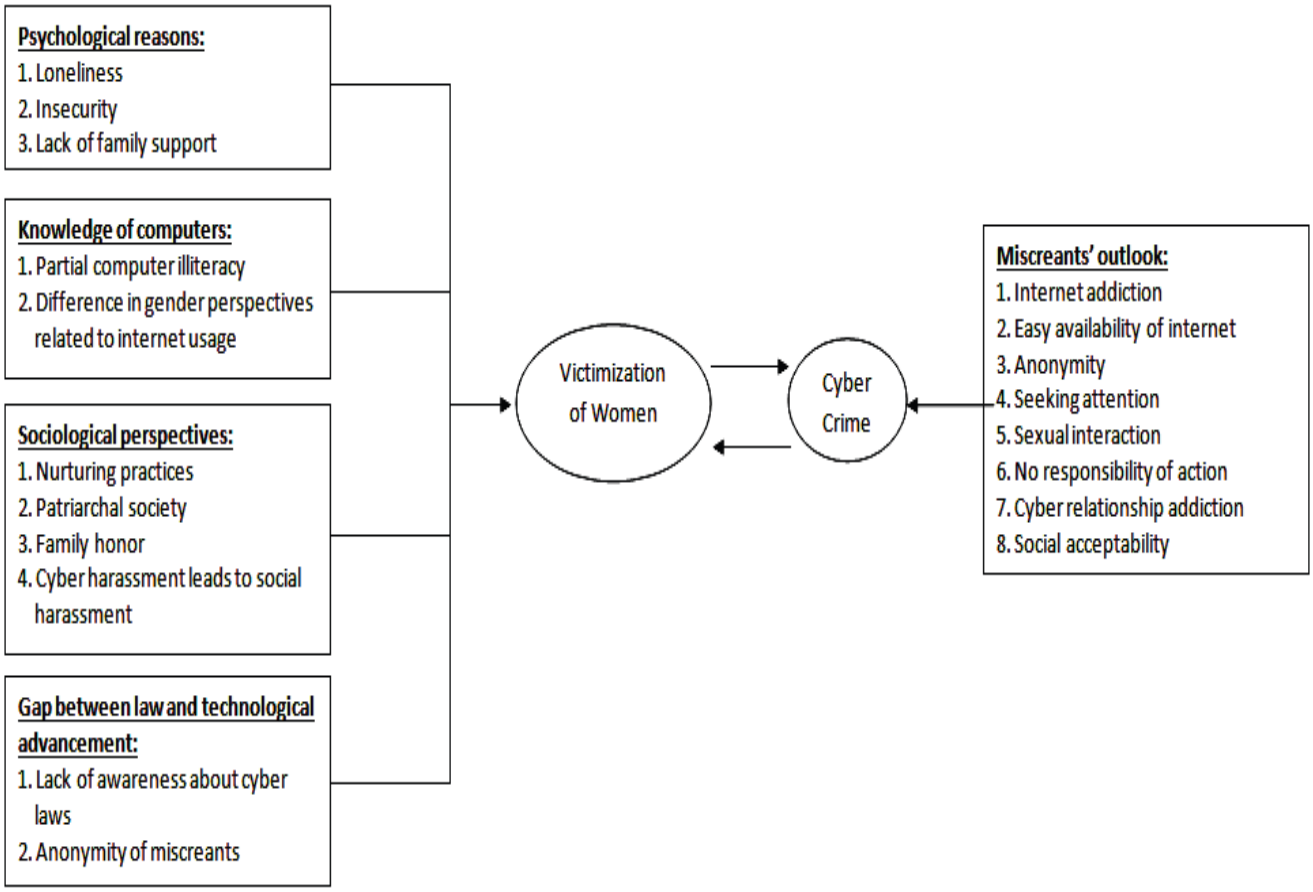
ISSN 2581 3382

 Maximum people are unaware that stalking or harassing any person over Internet can also invite penal actions. They do not know that there exist certain remedies for these kind of offences.

 Many people do not report their case of victimization in the cyber wing. This is the reason women are more prone to cyber victimization as they fear loss of their reputation.

 Expressing of their opinions about various actions brings them to the light especially women. They are targeted and are replied with hate messages and emoticons which make them feel unsafe and threatened.

Consequences of these crimes



Cyber-crimes are not only crimes against the individual person but also against the entire society. It makes the person unsafe and harms his reputation among the right thinking members of the society. This also has psychological impact over the person. He is exposed to a sense of fear and is unable to face the outer world.

ISSN 2581 3382

- When there is identity theft and misuse of personal information, the person losses his reputation. He also may suffer some monetary loss and may result in loss of service and consortium.
- Women may feel unsafe even to communicate with another person. Cases of voyeurism and pornography are perfect examples for the same.
- Morphing and cyber stalking may result in loss of productivity of a person.
- Time is wasted in finding the root cause of the crime and the person stays under trauma. It also may affect his physical as well as psychological condition.
- It also results in IPR infringement and piracy.

What are the laws for protection?

The above named crimes are usually dealt by the Information Technology Act,2000 and the Indian Penal Code,1860.

Provisions under the Information Technology Act,2000:-

- Sec-43 of the Information Technology Act,2000 ,mentions about the compensation for the failure to protect data. It states that when a body while dealing or handling any sensitive personal is negligent which thereby causes wrongful loss or wrongful gain to any other person is liable to pay damages by way of compensation to the victim.
- Sec-44 of the Information Technology Act,2000 mentions about the penalty to be paid in case of failure to furnish information, return, etc. If a person fails to furnish any document, return or report shall be liable to penalty not exceeding one lakh and fifty thousand rupees for such failure. If the person fails to furnish the information, books or other documents within the time specified shall be liable to a penalty not exceeding five thousand rupees for every day. If the person fails to maintain books of accounts of records shall be liable to pay ten thousand on daily basis till the failure continues.
- Sec-63of the Information Technology Act,2000 states that if any person dishonestly or fraudulently does any act which may lead to wrongful gain or wrongful loss to a third person shall be punishable with imprisonment for a term which may extend upto three years or with fine which may extend upto five lakh rupees or both.
- Sec-66 of the Information Technology Act,2000 mentions that whoever commits hacking shall be punished with imprisonment upto three years or fine upto two lakh rupees or both.

ISSN 2581 3382

- Sec-66A of the Information Technology Act,2000 states punishment for the sending of offensive messages with imprisonment for a period which may extend upto three years and wit fine.
- Sec-66B of the Information Technology Act,2000 states that in case of dishonestly receiving or retaining any stolen computer the person may be punished with imprisonment for a term which may extend upto three years or with fine upto one lakh rupees or both.
- Sec-66C of the Information Technology Act,2000 which includes identity theft shall be punished with imprisonment upto three years or with fine upto one lakh rupees or with both.
- Sec-66D of the of the Information Technology Act, 2000 states that whoever by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment upto three years and liable to fine upto one lakh rupee.
- Sec-66E and Sec-72 of the Information Technology Act,2000 respectively provides for punishment for the violation of privacy and breach of confidentiality and privacy. The person shall be liable to punishment upto three years or with fine upto two lakh rupees or with both.
- Sec-67 of the Information Technology Act,2000 provides for punishment for publishing or transmitting obscene material in electronic form with punishment upto three years or fine upto five lakh rupees. And in the second conviction with imprisonment upto five years and fine upto ten lakh rupees.
- Sec-67 A deals with the punishment relating to cyber pornography. In case of publishing or transmitting material containing sexual content, the publisher shall be punished with imprisonment upto five years and fine upto ten lakh rupees. In the event of second conviction with imprisonment upto seven years and fine upto ten lakh rupees.
- Sec-67 B provides for punishment of material depicting children in sexually explicit act with imprisonment upto five years with fine upto ten lakh rupees and in the event of second conviction with imprisonment upto seven years or fine upto ten lakh rupees.

Provisions under Indian Penal Code,1860:-

ISSN 2581 3382

- Section 292A of the IPC[17] provides with punishment for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, with imprisonment upto 2 years or fine of two thousand rupees in first attempt. For second conviction it provides for imprisonment upto 5 years and punishment upto five thousand rupees.
- Under Section 509 of the IPC there is punishment for uttering any word or making any gesture intended to insult the modesty of a woman with simple imprisonment for a term of three years and also with fine.
- Under Section 293 of the IPC, there is punishment for the selling; distributing, circulating, etc. of any obscene material to any person below twenty one years shall be punished with imprisonment upto three years with a fine of two thousand rupees on first attempt. And on second even of conviction there is punishment for a period of five years and fine upto five thousand rupees.
- Section 354 C provides punishment of voyeurism with imprisonment for one year which may extend upto three years and shall be liable for fine in first attempt. And in second attempt the person shall be punished for at least three years which may extend upto seven years and shall be liable of fine.
- Section 354 D provides for the punishment of stalking with imprisonment for a period of three years and fine on first attempt. On the second conviction it implies imprisonment for a term of five years and fine.

Provisions under International Law:--

- Article-12 of the Universal Declaration of Human Rights (1948) provides for the protection of privacy of person and has provisions of punishment for any interference and attacks.
- Article-17 of the International Covenant on Civil and Political Rights protects any person and his data against arbitrary interference and has punishments for such interference.
- Article- 8 of the European Convention of Human Rights states that everyone has a right to respect his privacy and any interference to such will attract punishment.

[17] Indian Penal Code 1860

ISSN 2581 3382

Whether these laws are sufficient?

The laws for the protection of a women in cyberspace are sufficient only and only when there is proper implementation of those laws. When maximum people are unaware that there exist certain laws for their protection then there can be no remedy available to them. There again arises the question that the laws if sufficient are sufficient on paper or in practice. Or there is requirement of any stringent laws for the same. Or there is need of stringent laws at the same time with proper implementation. Also there lies a very large gap between the legal actions and technical development. Our cyber specialists are not always ready to know the root cause and are not equally developed to know it.

Recommendations

I. Changing passwords from time to time: It is very well known fact that we prefer easy password because they are simpler and easy to remember too. To lower the risk of hacking and other cybercrimes it is very much essential to give a strong password and keep the password changing from time to time. This in turn will secure the account as well as the system from getting affected. Strong passwords should be given in such a way that they are not easy to guess and can secure all personal details and other devices including cellphones, emails, banking details, credit cards, etc. Even secret questions should not be easily answered as they may result in leak of the private detail.

II. Avoid revelation of home address: There are many people who reveal their address over social networking sites and other working portals. Out of which the women are targeted and victimized. Their actions and movements are followed and they are harassed and threatened. This rule should specially be applied to the women who work as business professionals. Instead of revealing their personal details they can keep that data privately or only for specified users. They can use their work address privately or can use them in case of inbox messages. It can help them avoid stalkers and their information will not be misused. There will be no data piracy or theft.

III. Maintain stable relationships: Every woman should maintain a stable relationship with the persons they know. It is not required to have 1500 friends in friends list rather only 150 friends which whom we have a stable relationship and they won't harm us any way.

ISSN 2581 3382

IV. Organizing awareness campaigns: Awareness campaign be organized at every institution from the grass root level and every person should be made aware of cybercrimes and their consequences. These campaigns can be productive for curbing cybercrimes.

V. Seminars and workshops for better understanding of cybercrimes: Various persons like police, lawyers, scholars, cyber world experts should be invited to the schools to make the students aware about cybercrimes. They should be made clear that not only girls can be targeted in cyberspace. Workshops and seminars should be organized to make everyone aware and there should be quick responses to the complaints lodged.

VI. Formation of rigid and stringent laws: There should be stringent laws made to protect the women from being victimized in cyber space. The laws made should be implemented in a proper way and there should be certain alterations brought in the legal system. The provisions should be altered and re-altered as per the need of the society.

VII. Do not answer unsolicited calls and messages: Woman should beaware of the spam messages and avoid unwanted or unsolicited phone calls. As their phone could be tapped and their movement could be followed by tracing the location. They should also download applications from trusted websites. In case there is any problem that should be discussed with parents and other trustworthy members of the family.

VIII. Knowledge of privacy settings: Women must have proper knowledge of the privacy setting over social media. They should not make their profile public as it may lead to intrusion of privacy. They should also adopt potential measures to suffer from online harm.

IX. Anti-Virus must be updated: The anti-virus must be kept up-to date. Because there can be Trojan worms, and other ways to inject virus that can be used to access the information of a person. In this way, the computer network and the computer system will stay protected and there will be no malfunction of data.

X. Check account actions: Our actions over the social networking sites must be checked regularly. There may be certain times where the account gets hacked and the victim has no knowledge about the same.

XI. Efficiency in Judiciary System: The main concern of the victimization of cyberspace is because of no certain boundaries or jurisdiction, loss of evidence, lack of cyber army and cyber

ISSN 2581 3382

courts to deal with such offences and crimes. So there is delay in providing remedy to the victim. So there should be major change brought in the field of technology and cyberspace.

Conclusion

Cybercrimes are not only rising in India but are a threat to the entire world. Innocent people having a little knowledge about the cyber world especially women are targeted and victimized. Many women have the fear of loss of reputation as a result of which they do not file a complaint against the offenders. So they escape and target other persons. Instead of being a victim they should come up as a strong personality and face the challenge. Firstly, they should overcome their own fear and fight for their rights. Secondly, the government should also bring on new laws not only on paper but also in practice. Thirdly,the person should also change their attitude towards women. They should not treat them simply as a commodity or a material but should rather treat her as a human being. Because the same women could be the mother, sister, daughter or wife of a particular person. They should develop the sense of commonality as cleanliness starts from home.

ISSN 2581 3382