CYBER CRIME IN INDIA WITH SPECIAL REFERENCE TO WOMEN, CHILDREN AND SENIOR CITIZENS

Written by ***Dr Sanskriti Mishra***

Assistant Professor, School of Law, Sharda University, Greater Noida, India

ABSTRACT

With the increasing use of computers in society, cybercrime has become a major issue. And now cybercrime is one of the most complicated issues of the cyber world. "Cybercrime is basically an illegal act in which a computer is either a tool/ mean or target". The evolution of the internet provides easy access to data and information from anywhere over the globe. Any person can access the information over internet from their any place in the world. However, there are some drawbacks also. Instead of being benefitted with the facilities of internet, some peoples tend to misuse the computers and internet for crime. There are different categories of have taken birth over internet as cyber pornography, cyber defamation, cyber bullying, cyber grooming, cyber stalking, email bombing, carding, cheating and fraud, virus attacks, web jacking, hacking etc. In this article, the author analyzed the easier access to internet and social media resulting in increasing cyber-crimes against women, children, and senior citizens in Indian society. There are several crimes known and unknown to normal person through which mostly women get victimized in way of Cyber staking, Harassment through e-mails, cyber-sex, Cyber defamation etc. and other than these crimes, crime minds use the cyber world's tools for child abuse which is also serious as it impacts the innocent minds of children. The crimes against the children using computer and internet are having different facets as exposure to sensitive content, possession, production and distribution of child pornography, cyber harassment, and sexual abuse, cyber bullying etc. Along with women and children, there is one more descendant who is easy target to cyber-attackers. Within the last decade, the number of senior citizens has been increased significantly among the internet users. It has been recorded in the past decade that senior citizen had the greatest rate of increase in Internet usages among

all other age groups. However, senior citizens are prone to be targeted and exploited by cyber criminals specifically for financial crimes.

In this paper, the researcher discussed the various categories of cybercrimes which are commonly imposed upon a woman, children and senior citizens, further the researcher analysed that how these crimes adversely affect them. The researcher also briefly examined the various laws for the protection of women, children and senior citizens; (i) Information Technology Act (2000), (ii) Constitutional liability, (iii) The Protection of Children from Sexual Offences (POCSO) Act, 2012, (iv) The Indian Penal Code (IPC), 1860

Lastly, the author focuses on the remedies available to the victims of cybercrime and the changes required in the legal system to effectively curb the rising spirits of cyber criminals.

INTRODUCTION

The invention of Computer has made the lives easier as it was never before; it has been using for various purposes starting from the individual to large organisations across the globe. Nowadays Internet is becoming part and parcel of a modern lifestyle of the people throughout the world. It is simultaneously empowering, fascinating, difficult, and dreadful. To most of the people, the Internet remains mysterious, forbidding, incomprehensible and frightening. Since decades, the majority of computer users have been misusing the technology, either for their own profit or that of others. This gave birth to “Cyber Crime”.

Every year on March 8, we celebrate International Women's Day to show our respect, love, admiration, and gratitude for women. Even in our traditional ancient Indian society, women were placed at a very high position, The Vedas revered women as a 'Devi' and praised them as the mother, the creator, and the one who gave birth. But now the situation is not so well. India being one of the worst countries in the world for the exploitation of women. Women and children are among the most vulnerable members of society, making them easy targets for cybercriminals. This was especially true during the epidemic, even though men and adults were also susceptible to numerous cybercrimes. For many decades and indeed today, women have been harassed in numerous ways. Domestic violence, Sati Pratha, acid-attack, rape, eve-teasing, sexual harassment, dowry death, molestation, kidnapping, honor-killing, female

infanticide etc. are some forms which come into the category of violence against women. In modern time women are viewed and portrayed as sex objects, she is inferior to men in our society, this has created a huge gender bias between the men and women where the has typical mentality that their wrongdoings towards women cannot be penalized. This gift of the internet is used by the criminally inclined to commit wrongdoing and then conceal themselves under the cover given by the internet. The cyber world in itself has a virtual reality where anyone may conceal or even fabricate his identity.

Everyone over the world has had a rough time during the pandemic. The COVID-19 virus has been shown to be a catastrophe that has killed many people and caused millions of others to suffer mentally, physically, and emotionally. Millions of individuals have lost their lives as a result of the pandemic. The most susceptible and straightforward targets of these cybercrimes have been children, especially those who have either been abandoned because they have lost both of their parents or who have been temporarily separated from them because one of them has contracted an illness. In today's society children are the most endangered section and as a result of their lack of majority level, they are readily exploited in the cyber world. Nowadays, it is observed that even child sexual exploitation has started online. Cyber Crime is growing day by day and a large group of individuals became victims of hacking, theft, cyber stalking, fraud, malicious software, child soliciting etc. 'There are two main forms of this behaviour. The first involves using the Internet to traffic and/or collect child pornography. The second involves the widely publicized problem Children of adult men soliciting sex from minors on-line'. When children are separated from their parents or have no one to care for them, they are more vulnerable. Children are readily tricked into engaging in immoral behaviour and making themselves easy prey for cybercriminals since they lack the knowledge necessary to determine whether a specific website is acceptable to visit or not, as well as whether a particular image or video should be downloaded or not. Because of this, it's quite simple for sexual predators and other cybercriminals to access these kids' gadgets and manipulate them.

Cybercrime is on the rise as more people across the world use the internet. Estimates for the amount of money people and businesses have lost as a result of online fraud range from 100 billion. Over the world, the number of adults over 60 has increased rapidly in last decades specifically during covid pandemic. Older adults are a fast-growing group of internet users. Like the rest of the population, the growing adoption of internet technology has exposed older

adults to threats of online crime. Although fraud affects people of all ages, older adults are disproportionately vulnerable. Older people were found to be attractive targets to criminals due to their perceived relative lack of familiarity with technology, relative wealth and hesitancy to report the crime to authorities due to feelings of shame.

LITERATURE REVIEW

1. **"Cybercrime against women and children", Aditi Shrivastava, 2021**

   In this article the author provided that with increasing the rate of internet uses, the rate of cybercrime increased incredibly during the lockdown in India. A total of 704 cyber-crimes registered against women in 2020 and 504 in 2021 (till July). Cyberstalking, Sextortion, Cyber-Hacking, Cyber-Bullying, Sexual Abuse (including the use of pornographic and sexually explicit material against the victim), Cybersex Trafficking, and Phishing are the most frequent cybercrimes performed against women during the pandemic. Cyberbullying, child grooming, cybersex trafficking, and sexual abuse of minors are among the most prevalent cybercrimes performed against children during the pandemic. Due to their vulnerability, women and children were particularly easy prey for cybercriminals and sexual predators during the lockdown.

2. **"Cyber Crime and the Victimization of Women: Laws, Rights and Regulations", Debarati Halder, 2011**

   Cyber Crime and the Victimization of Women: A distinctive and significant addition to the literature examining several facets of cybercrime is Laws, Rights and Regulations. This book deals directly with a topic that is typically only mentioned incidentally, i.e. as a side effect of a particular cybercrime instance or concern. It investigates the gendered aspects of online crimes such cyberbullying, cyberstalking, defamation, modified pornographic photos, and electronic blackmail. Perpetrators who, for a variety of reasons, are unlikely to be identified or punished routinely use these and other methods to intimidate, control, and cause other harms. Researchers, academics, legislators, everyday women, and those who support them will learn more about cybervictimization and how to better respond to cybercrimes against women.

3. **"Everything about cybercrimes against women", A. Thiruthi, 2021**

   In this article the author summarises, while a crime-free society is impossible to achieve and only exists in fantasy, it should be a continuing effort to enforce regulations that reduce criminality to a minimum. Particularly in an increasingly technologically reliant world, criminality related to electronic law-breaking is certain to increase, and legislators must go the extra mile to keep impostors at bay. Technology is often a double-edged sword that can be employed for either good or evil purposes. To combat cybercrime against women, the Legal system has enacted a number of legislations. Thus, it should be the relentless efforts of rulers and legislators to assure that technology advances in a healthier way and is employed for legal and ethical economic growth rather than criminal activity.

4. **"Internet crimes against children", Keith F Durkin, 2012**

   Internet crimes against children are a contemporary social problem which has drawn a great deal of attention from the parents, educators, legislators, and law enforcement officials. This phenomenon has captured national attention in the United States with a number of media reports of this phenomenon. These crimes include child pornography offenses, as well as adults soliciting minors for sexual purposes on line. Drawing upon data from recent national surveys, the characteristics of offences, offenders, and victims are examined. A multitude of issues related to the assessment and classification of the individuals who commit Internet crimes against children are also explored. Strategies for the prevention of this behaviour and enforcement of laws protecting children online are discussed.

5. **"Older people's experience of cybercrime victimisation in Mumbai", Kartikeya Tripathi, 2019**

   In this brief report, the author described possible vulnerability factors for cybercrime among older people in Mumbai, as well as the potential impact of this crime. Report draws on the limited, existing literature on cybercrime and older people in LMIC and uses qualitative interviews with older people who have been victims of cybercrime in Mumbai and their supporters to illustrate and add to these findings. The sample size was small but suitably diverse for the first exploratory study of this nature. It was difficult for the researchers to recruit participants without convenience sampling in near

total absence of official data on the subject. However, the final sample included victims of three most common types of cybercrime in Mumbai and their relatives. The experts interviewed represented the views of the major institutions—police, the legal system, investigators and Non-governmental organisations—who interact with older people who are victims of cybercrime. The perspectives author present highlights the importance of data protection in preventing online fraud, the need to provide older people, who constitute a high risk group, with the skills, awareness and tools to take precautions in sharing their private information and training of frontline staff in banks, phone companies and police stations on how to avoid data leaks and support victims when crimes occur. These preliminary findings can inform larger studies to support the design of safeguards for older, internet users in LMIC; as well as training for staff of banks and police on how to respond to older people reporting cybercrime.

6. **P. K. Vanita, (2012)**, has concentrated on the various issues related to the first-level and second-level technical knowledge of cybercrimes for detection, prevention, and investigation of cybercrimes against women. These issues relate to the prevention, investigation, prosecution, and punishment of cybercrimes by Indian law enforcement authorities.
7. **Virendra Kumar, (2018)**, has discussed the different types of cybercrimes committed against women. Author has pointed out that, increase in the users of Internet, there is an increase in cybercrime rate. Author has opined that victimised women should come forward and report against the crime in a special Anti-cyber crime cell. In the opinion of the author, awareness among women about cybercrimes, and usage of the Internet, social media will definitely help to curb the cybercrime, and there will be reduction in the cybercrimes.
8. **N. Agarwal, (2014)**, has discussed cyber crimes and outlined security vulnerabilities against women in India. Through the study the author has also understood the opinions/ perceptions of police officials, counsellor's cyber cell officials etc. about the cyber-crimes against women. Author has also discussed the Information Technology Act 2000.

UNDERSTANDING CYBER CRIME

Cybercrime is the term commonly used for illegal activities which can be done by using a computer and internet as its primary tools for commission. It is an offence when someone or a group of people uses contemporary telecommunication networks like the Internet to purposefully damage the victim's reputation or cause the victim's physical or mental harm either directly or indirectly. Women, children, and older citizens who are unfamiliar with the online world and have just recently begun using it are particularly vulnerable to falling for the traps set by online bullies and fraudsters. The following are the most common sorts of cybercrimes and cyberbullying that are committed online:

Cyber-crime against women

Women are considered soft target to be manipulated. Also lack of knowledge about the complexities of internet world, less exposure, lack of awareness are some key points which makes them prone to be target by criminal minds. Here are some categories of cybercrimes against women as;

- **Cyberstalking**

  It included connecting or trying to connect with the victim on social media or phone calls despite clear indication of disinterest from her end, posting messages (sometimes threatening) on the profile of the victim, constantly bombarding the victim with emails/text messages/phone calls, etc.

- **Sextortion**

  This is the most common cybercrime committed against women during the period of the pandemic. The offenders started extorting money or sexual favors by blackmailing the victims to reveal their private pictures or morphed images. The pandemic and lockdown frustration made the offenders seek sexual video calls/images or messages from women by threatening them. Also, loss of income encouraged them to extort money by threatening the victim with their morphed images.

- **Cyber hacking**

During the lockdown, people started to read news online. There was a rise in cases of fake news and information. The women started becoming the victim of cyber hacking by clicking on malware links which get all their information available on phone, turns on the camera and microphone, and captures their intimate pictures and videos. Offenders, in turn, use these pieces of information and pictures for sextortion and other favors.

- **Cyberbullying**

This included publishing defamatory and abusive statements against the victim on social media platforms and demanding money for deleting them, insensitive comments on the posts of the victim, exchanging morphed images/private images of the victim without her consent, sending rape threats to the victim, etc.

- **Phishing**

To make money in lockdown, offenders are sending fake emails with a link to a particular webpage to induce the victim to unwittingly enter personal data like bank account details, contact details, and passwords or with the intention to install harmful viruses in the victim's device as soon as they open the link. These emails and messages appear to have come from legitimate sources. The offenders then make fraudulent transactions from the victim's account to their account with the use of the bank account and other personal details of the victim.

- **Sexually abusive and pornographic content**

During the pandemic, offenders were also indulged in sexual abuse of women on the internet, morphing the picture of the victim and using it for the purpose of pornography.

- **Cybersex trafficking**

Unlike sex trafficking, the victim does not come in direct contact with the abuser. In cybersex trafficking, the dealer live-streams, films, or photos of the victim performing sexual/intimate acts from a central location and sells the material online to sexual predators and buyers. The offenders have been sexually abusing women by making them a part of cybersex trafficking byways of coercion, manipulation, and blackmailing.

Cyber-crime against children

Children and teenagers are next soft target to get in box easily. Here are some common forms of cyber-crimes against children which are described, they are;

- **Sexual abuse of children**

This includes child sexual abuse materials such as child pornographic images and videos, online sexual exploitation of children over phone call/video call where children are coerced into performing sexual acts.

- **Pornographic/sexually explicit content for children**

While using the internet for education and entertainment purposes or going through a social media page, children are being induced to open certain websites which direct them to sexually explicit content and pornographic videos/images. This corrupts the mentality of the child but the offender gets views and money.

- **Cybersex trafficking**

Unlike sex trafficking, the victim does not come in direct contact with the abuser. In cybersex trafficking, the dealer live-streams, films, or photos of the victim performing sexual/intimate acts from a central location and sells the material online to sexual predators and buyers. The offenders have been sexually abusing children by making them a part of cybersex trafficking byways of manipulation and coercion.

- **Cyberbullying**

This includes harsh, mean, abusive, or cruel comments and messages against the child victim. Children are easy to bully because of their innocent nature and it becomes even much easier for the offenders to bully children on virtual platforms. Cyberbullying causes; avoiding school classes via virtual platforms, suddenly wanting to stop using the internet and computer devices, being secretive about their digital life, distress, and emotional instability among children.

- **Child grooming**

The offender befriends the child victim by forming an emotional and fiduciary bond with him/her with the objective of sexual abuse of the child. The children tend to trust easily and hence, it becomes very much easy for the offenders to create such a bond with them. Once the bond is created, the offender starts manipulating the child to perform sexual acts. Child grooming via online platforms and social media has been one of the most committed cybercrimes during the pandemic. Child groomers were able

to operate and gain children's trust online and it became easy for them to do so because of the unawareness of children and parents about the dark side of the internet world.

Cyber-crime against senior citizens

Due to age factor the learning and memorizing capability becomes lesser. And it became a good opportunity to cybercriminals. Some of the tactics of cyber criminals which they used to trap senior citizens are like;

- Deliberately spreading fraudulent reverse mortgage and loan offers.
- Pressuring elderly to pay in full or in part up front for services rendered by unregistered contractors. These thieves frequently never start or complete the work, costing the victims more money.
- Coercing senior citizens to provide their financial or personally identifying information (PII) in order to open new accounts.
- Pretending that family members creating credit cards in the victims' names or stealing money from their accounts.
- Charging fraudulent or unnecessary services using elderly victims' Medicaid or Medicare information.
- Targeting seniors with get-rich-quick pyramid schemes, or telling victims they've won a contest or the lottery. To collect, all they need to do is transfer a "small" amount of money to an account and then their winnings will be transferred to them.
- Influencing elders to make erroneous purchases, such as a coffin for a departed spouse when they will be cremated, by misleading them into doing so

These are just a few examples – the list goes on and on. While there are many other types of senior fraud, here are a few of the most common:

GENERAL STRATEGIES OF CYBER-CRIME FOLLOWED BY CYBER-CRIMINALS

Strategy 1: Online and Telephonic Phishing Scams

Everyone loves a good deal and women, seniors and children are natural soft target for that. Therefore, they are at top of the list of cyber attackers. They used to get frequently phone calls and emails with hidden scams or hidden cyber viruses. Free gifts vouchers, prizes, reward points, low-cost medications, low-cost goods and services and other items that seems good to be true (because they are). The criminals use these items and other interests as bait in a type of attack known as phishing.

Phishing typically refers to schemes that fool victims into supplying a range of personally identifying information (PII), bank account information, and login information through the use of unsolicited mails. Tactics often include the use of social engineering and language that evokes an emotional reaction such as fear or curiosity. Phishing can occur via email, over the phone (voice phishing, or "vishing"), and via SMS (SMS phishing, or "smishing").

Strategy 2: Identity Theft

People of all ages, colours, and socioeconomic backgrounds are victims of identity theft. It also takes many different forms, such as Social Security theft, tax refund theft, and medical identity theft. Online, over the phone, or by just obtaining the victim's information, identity theft can take place.

Strategy 3: Confidential Fraud

For many children and seniors, the internet represents a less intimidating way to connect with and meet new people. But this is also the playground of cybercriminals. These malicious actors use online platforms and other methods to conduct highly targeted attacks.

An elderly victim in this crime is tricked into thinking they have a relationship built on trust with the actor. This connection is used by the criminal, who may pose as the victim's grandchild or romantic interest, to influence the victim to:

- provide personal and financial information.
- give money or buy expensive gifts; or
- launder money unknowingly.

This particularly heinous cybercrime most commonly targets elderly women and those who are recently widowed.

REASONS FOR RAPID GROWTH OF CYBERCRIME

'Human beings are vulnerable, so rule of law is required to protect them' – Prof Hart said in his work "The Concept of Law". If we extrapolate this to the cybersphere, we may say that because of computers' vulnerability, the rule of law is necessary to defend and safeguard them from cybercrime. The causes of computers' susceptibility to attack include:

- **Easy access to everyone-** The difficulty in protecting a computer system from unauthorised access is that there is always a chance of a breach caused by complex technology rather than by human error. Key loggers that can steal access codes, sophisticated voice recorders, retina imagers, and other devices that can trick biometric systems and get beyond firewalls can be used to get past numerous security systems by being covertly implanted with logic bombs.
- **Negligence-** Negligence and human behavior are intimately related. Therefore, it is extremely likely that any negligence that occurs when safeguarding the computer system will allow a cybercriminal to access and take control of it.
- **Complex-** The human mind is flawed, thus it's unlikely that there won't ever be a mistake. The computers work on man-made programs which are commands/instructions which are composed of millions of codes. Sometimes user-friendly interface too has a lot of options and hidden tabs make the system operating tuff to handle.
- These holes allow the computer system to be breached by cybercriminals.

THE REMEDIES AVAILABLE FOR VICTIM OF CYBER CRIME

Cyber Crime complaint registration

Any of the following ways can be used by the victim of cybercrime to file a complaint:

1. National Cybercrime Reporting Portal (Online Cyber Crime complaint);
2. Cyber Crime Cell (Offline Cyber Crime complaint);
3. Local Police station (Reporting of cyber-crime)

However, The National Cyber Crime Reporting Portal has been the easiest and most practical

way to file a complaint about cybercrime during the pandemic. The victim won't need to go to a police station or a cybercrime cell to complete the necessary paperwork or submit the proof.. The victim can easily file a complaint about the crime perpetrated against her using this way while sitting in her home. When filing a complaint, the pertinent evidence may also be uploaded to the Cybercrime Portal. Additionally, the victim will have the ability to monitor the progress of her complaint using the registered mobile number. Cybercrime offenses against women and children such as "Child Pornography, Child Sexual Abuse Material containing sexually explicit images/videos of children, sexually explicit content such as rape/gang rape" etc. can be registered by the victim/complainant on the Cybercrime portal. The relevant material may also be uploaded to the Cybercrime Portal when submitting a complaint. Additionally, using the registered mobile number, the victim will be able to follow the development of her complaint. Additionally, the victim or complainant has the option of registering the complaint anonymously, in which case their identify will not be made public. The victim/complainant must select the "Report and Track" option and register with a mobile number and email address in order to check on the status of the complaint in the future. With this choice, the victim or complainant will be promptly informed of any inquiries made and measures taken by the police officer in relation to the complaint filed.

The offline technique, in which the victim can send a written complaint to the closest cybercrime cell addressed to the Head of that particular cybercrime cell, is another choice available to the victim for the registration of a cybercrime complaint. The victim's name, contact information, postal address, and any further pertinent documents or evidence must be included with the complaint application.

If the victim or complainant does not have access to any of India's cybercrime cells, internet services, or devices, he or she may still register a FIR at a nearby police station with all the necessary details and supporting documentation.

Information Technology Act, 2000

Provides the provisions related to. Cybercrime as:

- **Section 66C** of the IT Act makes identity theft a punishable offence. "Instances of cyber hacking would be covered by this provision. Under this provision, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
- **Section 66E:** Punishment for violation of privacy

  This section punishes the offender who intentionally or knowingly captures, publishes, or transmits the image of a private area of any person or a person engaged in private activities without the consent of such person.

  Punishment: Imprisonment which may extend to 3 years or fine which may extend to two lakh rupees, or with both.
- **Section 67:** Punishment for publishing or transmitting obscene material in electronic form

  This section punishes the cybercrime offender who publishes or transmits in the electronic form, any material which;

1. Is lascivious (capable of arousing sexual desire), or
2. It tends to deprave and corrupt the persons who are likely to read, see or hear the matter contained in it.

Punishment: First conviction- Imprisonment which may extend to 3 years and fine which may extend to 5 lakh rupees.

Second/subsequent conviction- Imprisonment which may extend to 5 years and fine which may extend to 10 lakh rupees.

- **Section 67A:** Punishment for publishing or transmitting of material containing the sexually explicit act, etc. in electronic form

  This section punishes the offender who publishes/ causes to publish or transmits/causes to transmit in electronic form any material which contains sexually explicit act or conduct.

  Punishment: First conviction- Imprisonment which may extend to 5 years and fine which may extend to 10 lakh rupees.

  Second/subsequent conviction- Imprisonment which may extend to 7 years and fine which may extend to 10 lakh rupees.

- **Section 67B:** Punishment for publishing or transmitting of material depicting children in the sexually explicit act, etc. in electronic form

  This section punishes the offender who publishes/causes to publish, or transmits/causes to transmit, or creates text or digital images, collects, seeks, browses, downloads, advertise, promotes, exchanges, or distributes any material, in electronic form which depicts children engaged in a sexually explicit act or conduct. It also punishes the offender who cultivates, entices, or induces children to online relationships with one or more children for a sexually explicit act, or who facilitates online abusing of children, or who records in any electronic form abuse or sexually explicit act with children.

  Punishment: First conviction- Imprisonment which may extend to 5 years and fine which may extend to 10 lakh rupees. Second/subsequent conviction- Imprisonment which may extend to 7 years and fine which may extend to 10 lakh rupees.

Indian Penal Code, 1860

Related provision is like;

- **Section 354A:** Sexual harassment and punishment for sexual harassment

This section punishes the offender who commits any of the following acts-

1. Physical contact and advances involving unwelcome and explicit sexual overtures;
2. A demand or request of sexual favors; or
3. Showing pornography against the will of the woman; or
4. Making sexually colored remarks.

Any of the above-mentioned acts if committed with the use of the internet, computer device, or computer network, amounts to cybercrime and is punishable under this section.

Punishment: Imprisonment which may extend to 3 years, or fine, or with both.

- **Section 354C:** Voyeurism

This section punishes the offender who watches or captures the image of a woman engaging in a private act when she believes and expects not to be watched or observed by the perpetrator or any other person.

Punishment: First conviction- Imprisonment which shall not be less than one year, but which may extend to 3 years and fine.

Second/subsequent conviction- Imprisonment which shall not be less than 3 years, but

which may extend to 7 years and fine.

- **Section 354D:** Stalking

This section punishes the offender who-

1. Follows a woman and contacts/attempts to contact such woman with the intention to establish a personal interaction despite clear indication of disinterest by such woman; or
2. Monitors the use by a woman of the internet, email, or any other form of electronic communication.

Punishment: First conviction- Imprisonment which may extend to 3 years and fine.

Second/subsequent conviction- Imprisonment which may extend to 5 years and fine.

- **Section 499**: Defamation

To defame a person is to do an act with the intention of harming the reputation of the person. Defamation by publication of visible representations of an imputation concerning the woman, when done with the intention to harm her reputation, is punishable with imprisonment for a term, which may extend to two years, or with fine, or both

- **Section 503**: Criminal intimidation

This section punishes the offender who threatens another with any injury to his person, reputation, or property with the intent to cause alarm to that person or to cause that person to do any act which he/she is not legally bound to do or to omit to do any act which that person is legally entitled to do.

Punishment under Section 506: Imprisonment which may extend to 2 years, or with fine, or with both. Punishment for criminal intimidation by imputing unchastity to a woman: Imprisonment which may extend to 7 years, or with fine, or with both.

- **Section 507**: Criminal intimidation by an anonymous communication

This provision provides the quantum of punishment for Criminal Intimidation when the same is by a person whose identity is not known to the victim. Any anonymous communication, which amounts to criminal intimidation under Section 503 stated above, is punishable under this section.

- **Section 509:** Word, gesture, or act intended to insult the modesty of a woman

This section punishes the offender who, intending to insult the modesty of a woman, utters any words, makes any sounds or gesture, or exhibits any object, or intrudes upon the

privacy of such woman.

Punishment: Imprisonment which may extend to 3 years and fine.

The Indecent Representation of Women (Prohibition) Act, 1986

- **Section 4**: Prohibition of publication or sending by post of books, pamphlets, etc., containing indecent representation of women.

This section 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.

Punishment under Section 5: First conviction: Imprisonment which may extend to 3 years and fine which shall not be less than fifty thousand rupees, but which may extend to one lakh rupees.

Second/subsequent conviction**:** Imprisonment which shall not be less than 2 years, but which may extend to 7 years and fine which shall not be less than one lakh rupees, but which may extend to five lakh rupees.

Protection of Children from Sexual Offences Act, 2012

- **Section 11**: Sexual harassment of child and punishment therefore

Under this section, the sexual harassment of children has been defined. Sexual harassment of a child is said to be committed when the offender-

1. Utters any words, makes any sounds or gesture or exhibits any object or part of the body with the intention harass such child; or
2. Makes a child exhibit his body or any part of his body so as it is seen by such offender or any other person; or
3. Shows any object to a child in any form or media for pornographic purposes; or
4. Repeatedly or constantly follows/watches/contacts a child either directly or through electronic, digital, or any other means; or
5. Threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or

6. Entices a child for pornographic purposes or gives gratification.

Punishment for sexual harassment of a child under Section 12: Imprisonment which may extend to three years and fine.

- **Section 13**: Using child for pornographic purposes and punishment therefore

Under this section, the offender who uses a child for sexual gratification, in any form of media (including Advertisement or Programme telecast by TV channels or internet or any other electronic/printed form), shall be guilty of the offense of using the child for pornographic purposes. The use of a child for sexual gratification includes-

1. Representation of sexual organs of a child;
2. Using a child engaged in real or simulated sexual acts (with/without penetration);
3. The indecent or obscene representation of a child.

Punishment under Section 14: First conviction- Imprisonment which may extend to 5 years and fine. Second/subsequent conviction- Imprisonment which may extend to 7 years and fine."

CONCLUSION AND SUGGESTIONS

The combating of the Cyber-crime can be done generally in three ways: Sensitization and awareness between the users, Use of Prevention and Detection tools, combating by the method of strong law and legislatures. Victimized community should directly contribute to the experience regarding prevention of the cyber-crime because the criminal strategies are absolutely new and mysterious trends of victimization. Now the need for some other gender related law that protects the common legal rights of women. Level of awareness of adult internet users of modern cyber cultures, Media interventions are the public awareness campaigns and other interventions delivered through television, radio, newspapers and other mass media. These can render an effective contribution in bringing about changes within the attitudes of the individuals towards gender norms. The media interventions are successful, when they seek to generate information in terms of the target audience.

There are some suggestive strategies to prevent Cyber-crime as;

- A significant contributor to crimes against women has been identified as sending private photos to friends and total strangers when chatting online. Avoiding such behavior is crucial.
- It is advised to avoid disclosing any personal information online in order to prevent cyber stalking.
- To minimize risks, remain up to date with technological and internet breakthroughs.
- Firewalls are an excellent first line of defense for stopping such intrusions. Make sure security checks are used safely. Always turn on the router's built-in firewall.
- It is prudent to maintain the privacy of the credit and debit card information at all costs. When in doubt about whether a transaction is real, verify with reputable sources
- Become familiar with the legal system and procedures related to such offences so that you can act quickly if you are ever caught.
- To ensure their protection and safety, empower and educate women and children and senior citizens with the necessary information and understanding about the prevalence of such heinous crimes in society.
- When dealing with such threats, use prudence and presence of mind. Avoid being a victim of fancies.
- The ideal strategy to combat these cybercrimes would be to take a cooperative perspective involving the ideas and actions done by the government and other legislative authorities to address such crimes.