

ever-changing environment. Technology advances & the shift to networked & cloud environments where anti-forensic methods can easily come into play, obliges professionals in the fields to keep up to date & revise continuously standard operating procedures.

I.IV. BIBLIOGRAPHY

LEGISLATIONS

- Indian Evidence Act, 1872
- Code of criminal procedure 1973
- Information Technology Act, 2000
- Police And Criminal Evidence Act, 1984
- Youth Justice and Criminal Evidence Act, 1999.
- Bankers' Books Evidence Act

WEBLINKS

- Margaret Rouse, *computer forensic* (Oct 15, 2018, 14:06)
([https://searchsecurity.techtarget.com/definition/computer-forensics.](https://searchsecurity.techtarget.com/definition/computer-forensics))
- National institute of Justice, *Digital evidence and forensics* (Oct 15, 2018, 14:21)
([https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx.](https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx))
- cyberlawsindia.net, *forensic science* (Oct 15, 2018, 14:40)
([http://www.cyberlawsindia.net/computer-forensics.html.](http://www.cyberlawsindia.net/computer-forensics.html))
- US-CERT, *What is computer forensic* (Oct 15, 2018, 14:42)
([https://www.us-cert.gov/sites/default/files/publications/forensics.pdf.](https://www.us-cert.gov/sites/default/files/publications/forensics.pdf))
- Liu Qian, Fredrik Höglin & Patricia Alonso Diaz, *computer forensic* (Oct 15, 2018, 14:43)
([https://www.it.uu.se/edu/course/homepage/sakdat/hto7/pm/programme/Forensics.pdf.](https://www.it.uu.se/edu/course/homepage/sakdat/hto7/pm/programme/Forensics.pdf))
- Radha Kishan, *Importance of Computer Forensics* (Oct 15, 2018, 14:52)
([http://EzineArticles.com/1116636.](http://EzineArticles.com/1116636))
- Forensic control, *Introduction to computer forensics* (Oct 15, 2018, 14:55)

- <https://forensiccontrol.com/resources/beginners-guide-computer-forensics/>.
- IEEE, *FUTURE OF DIGITAL FORENSICS FACES SIX SECURITY CHALLENGES IN FIGHTING BORDERLESS CYBERCRIME AND DARK WEB TOOLS* (Oct 15, 2018, 15:01)
(<https://publications.computer.org/security-and-privacy/2018/03/01/digital-forensics-security-challenges-cybercrime/>.)
 - Willow Dawn Becker, *10 MODERN FORENSIC SCIENCE TECHNOLOGIES* (Oct 15, 2018, 15:05)
(<https://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies>.)
 - Ben Cole, *evidence in court* (Oct 15, 2018, 15:06)
(<https://searchcompliance.techtarget.com/feature/Governance-needs-shift-as-digital-evidence-in-court-becomes-common>.)
 - Vangie Beal, *Cyber Forensic* (Oct 15, 2018, 15:10)
(https://www.webopedia.com/TERM/C/cyber_forensics.html.)
 - Computer forensic NZ, *What is computer forensics?* (Oct 15, 2018, 15:14)
(<https://www.datarecovery.co.nz/forensic-investigation/what-is-computer-forensics/>.)
 - Finjan Team, *The Importance of Digital Forensics* (Oct 15, 2018, 15:19)
(<https://blog.finjan.com/the-importance-of-digital-forensics/>.)
 - Lori M Camron, *FUTURE OF DIGITAL FORENSICS FACES SIX SECURITY CHALLENGES IN FIGHTING BORDERLESS CYBERCRIME AND DARK WEB TOOLS* (Oct 18, 2018, 9:44)
(<https://publications.computer.org/security-and-privacy/2018/03/01/digital-forensics-security-challenges-cybercrime/>.)
 - FADI ABU ZUHRI, *Challenges faced by Cyber Forensic Investigator – Concepts and Techniques* (Oct 18, 2018, 09:55)
(<https://digitalforensicmagazine.com/blogs/?p=2197>.)
 - Kirankumar Akate Patil, Shrinivas Vyawahare, Kiran Shejul & Madhuri Girase, *Hurdles in Cyber Forensic Investigation in India*, IOSR-JCE, pg. 18-22

- (<http://www.iosrjournals.org/iosr-jce/papers/Conf.17003/Volume-2/4.%2018-21.pdf>.)
- Samarth, *Cyber Forensics & Electronic Evidences: Challenges In Enforcement & Their Admissibility*(Oct 16, 2018, 13:45)
(<http://www.legalservicesindia.com/article/975/Cyber-Forensics-&-Electronic-Evidences:-Challenges-In-Enforcement-&-Their-Admissibility.html>.)
 - Radha Rani, *Challenges of Digital Forensics in Cloud Computing Environment* (Oct 16, 2018, 13:50)
(<http://www.indjst.org/index.php/indjst/article/view/93051>.)
 - Ankita Lahiri, *Cyber forensic facility in India is inadequate*(Oct 16, 2018, 13:52)
(<https://www.governancenow.com/views/interview/cyber-forensic-facility-india-inadequate>.)
 - Ram Kumar, *forensic science* (Oct 16, 2018, 13:58)
(<http://computerforensicsinindia.blogspot.com/>.)
 - Jennifer Williams, *What Is Cyber Crime? - Definition, Types & Examples* (Oct 15, 2018, 17:48)
(<https://study.com/academy/lesson/what-is-cyber-crime-definition-types-examples.html>.)
 - BEDFORSHIRE POLICE, *what is cyber crime* (Oct 15, 2018, 17:55)
(<https://www.bedfordshire.police.uk/information-and-services/Crime/Cyber-crime-and-online-safety/What-is-cyber-crime>.)
 - Cybercrime.org.za, *Hacking Definition*(Sep 27,2018,14:18)
(<http://cybercrime.org.za/hacking/>)
 - Margaret Rouse, *Logic Bomb(Slag Code)* Sep 27, 2018, 14:41)
(<https://searchsecurity.techtarget.com/definition/logic-bomb>.)
 - imperva incapsula, *phishing attacks* (Sep 27, 2018, 14:57)
(<https://www.incapsula.com/web-application-security/phishing-attack-scam.html>.)
 - thechopedia, *email bomb* (Sep 27, 2018, 15:01)
(<https://www.techopedia.com/definition/1655/email-bomb>.)
 - KANIKA SETH, *WEB JACKING*, (Sep 27, 2018, 15:03)

- (<http://www.karnikaseth.com/what-is-web-jacking.html>.)
- Margaret Rouse, *CYBER STALKING* (Sep 27, 2018, 15:06)
(<https://searchsecurity.techtarget.com/definition/cyberstalking>.)
 - Tanushree Sharma, *What is Data Diddling* (Sep 27, 2018, 15:09)
(<https://www.legistify.com/QnA/answer/1920-what-is-data-diddling>.)
 - CK STAFF, *What's the difference between credit card fraud and identity theft?* (Sep 27, 2018, 15:13)
(<https://www.creditkarma.com/credit-cards/i/credit-card-fraud-identity-theft/>.)
 - Techopedia, *what is software piracy* (Oct 7, 2018, 20:21)
(<https://www.techopedia.com/definition/4361/software-piracy>.)
 - Daniel Brecht, *computer crime investigation using forensic tools and techniques* (Oct 15, 2018, 18:31)
(<https://resources.infosecinstitute.com/computer-crime-investigation-using-forensic-tools-and-technology/#gref>.)
 - Felix C. Freiling, *A Common Process Model for Incident Response and Computer Forensics*. (Oct 15, 2018, 18:39)
(<https://pdfs.semanticscholar.org/ffec/5abbo2dd451643b190c2bfoffbd610666689.pdf>.)
 - NFSTC, *a simplified guid to digital evidence* (Oct 15, 2018, 18:54)
(<http://www.forensicssciencesimplified.org/digital/how.html#top>.)
 - X WAYS, *X-Ways Forensics: Integrated Computer Forensics Software* (Oct 08,2018, 00:56)
(<http://www.x-ways.net/forensics/>.)
 - guidance software inc, *Encase* (Oct 08,2018, 09:39)
(<https://www.guidancesoftware.com/>.)
 - GIAC Directory, *the coroners kit* (Oct 08,2018, 09:43)
(<https://www.giac.org/paper/gsec/2074/introduction-coroners-toolkit/100965>.)
 - Martin Brinkmann, *Computer Online Forensic Evidence Extractor* (Oct 08,2018, 10:05) (<https://www.ghacks.net/2008/04/29/computer-online-forensic-evidence-extractor/>.)

- Kali tools, *Bulk-extractor* (Oct 08,2018, 10:18)
(<https://tools.kali.org/forensics/bulk-extractor.>)
- Cherly A Purdy, *Registry Recon*(Oct 08,2018, 10:25)
([https://www.forensicfocus.com/c/aid=156/reviews/2016/registry-recon/.](https://www.forensicfocus.com/c/aid=156/reviews/2016/registry-recon/))
- Jack M. Germain, *CAINE Provides Sturdy Support for Forensic Specialists*,(Oct 08,2018, 10:33) (<https://www.linuxinsider.com/story/81353.html.>)



CYBER CRIMES AGAINST WOMEN

| Authored By : Ms. Priyanshi Chandrawat |
| Indore Institute of Law, Indore, Madhya Pradesh |

Cyber World is a need of an hour. It connects all the countries via technology. Cyber is all about online use of technology without manual labour but with smartness, intelligence & mindfulness.

No space is left without crime today. Same goes for cyber space & World. Various types of crimes are committed but cyber-crimes against women are specifically not dealt in the IT Act 2000.

Various cyber-crimes against women are as follows harassment via e-mails, cyber stalking, cyber pornography, defamation, morphing & email spoofing.

Let's take an example of Kerala state:

The NCRB (2012) figures gave an interesting insight into the changing mind-set of Kerala State: in 1996, cases registered under cyber crimes, were related to harassment of women. 48 cases were for committing fraud or illegal gain, 44 cases were for money, 19 for causing disrepute to others. Out of 312 persons arrested as suspects in cases for cyber crimes. 73 were neighbours, friends or relatives.⁸⁸.

NCRB (2012 statistics) for Kerala State regarding arrests for cyber crimes: 15 persons were below age of 18, 81 persons aged 18-30 years, 44 persons aged 30-45 years & 11 persons were 45-60 years. Out of the cases registered under IT Act in the Kerala State, 147 were for publishing or electronic transmission of obscene material, which is the highest among other States. Maharashtra came second with 76 cases.⁸⁹

⁸⁸ Cyber safety for Women, Lina Acca Mathew, Assistant Professor , Government Law College, Ernakulam

⁸⁹ *Ibid*

However, in modern times women are viewed and portrayed as sex objects, she is treated inferior to men in various societal spheres and functions, this has created a huge gender bias between the men and women where even the men think that their wrongdoings towards women cannot be penalised. Cybercrime and internet bullying works in similar manner where the wrong-doers are not afraid of any authority that can penalise.

The cyber world in itself has a virtual reality where anyone can hide or even fake his identity, this gift of internet is used by the criminally minded to commit wrongful acts and then hide under the blanket provided by the internet. The transcendental jurisdiction of Internet causes the major threat to the society in the form of cybercrime. The main victim of this transgression can be considered women and children. Studies shows that we have 52 million active internet users in India which reached at 71 million in the year 2009. Among them working women net users are 8% and 7% nonworking women in the year 2009 and 37% usage of all users accessing internet through cyber cafe. It is very common occurrence that the essential data of the internet surfer is being released effortlessly by the owners of cyber cafe and then it is used for illegitimate dedications. Though acquaintance with technology is constructive facet that can be considered vital for the progress of any country but at the same time it is becoming the foundation to upsurge the offense rate with technology against the weaker sector of the society. Statistics also show that cyber awareness amongst people in India is really low.⁹⁰

The reasons for the growth of cybercrime rate against women can be categorized into two folds: legal and sociological reasons.

Legal Reasons: The objective of the IT Act is crystal clear from its preamble which confirms that it was formed largely for improving e-commerce hence it covers commercial or economic crimes i.e. hacking, fraud, and breach of confidentiality etc. but the drafters were unacquainted with the protection of net users. As we deliberated

⁹⁰ Rajat Mishra, Cyber Crimes against Women, 15:10:2018, 12:00PM, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2486125,

above that majority of cybercrimes are being prosecuted under Section 66 (Hacking), 67(publishing or transmitting obscene material in electronic form), 72(breach of confidentiality). The most of the cybercrimes other than e-commerce related crime are being dealt with these three sections. Cyber defamation, cyber defamation, email spoofing, cybersex, hacking and trespassing into one's privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for instance modesty of women is protected under Section 509 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences and prosecuted under IPC. Indian constitution guarantees equal right to live, education, health, food and work to women, however until recently there were no specific penal provisions protecting women specifically against internet crimes. Ever since the 2012 Delhi Gang Rape case (Nirbhaya Case) there has been a huge outcry over bringing out new reforms and penal provisions so as to protect women against the criminally minded. The 2013 Criminal Law Amendment Ordinance contains several additions to the Indian Penal Code, such as to sections 354, 354 A, 354 B, 354 C & 354 D, with the assistance of these sections now the issues of MMS scandals, pornography, morphing, defamation can be dealt in proper manner. ⁹¹

As it has been discussed earlier that transcendental nature of Internet is one of the main reasons for the growth of cybercrime so whereas Section 75 of the IT Act deals with the offences or contravention committed outside India but it is not talking about the jurisdiction of the crimes committed in the cyberspace specially the question of place for reporting the case arises when the crime is committed in one place affected at another place and then reported at another place. Although in the most of the cases, for the matter of territorial jurisdiction Criminal Procedure Code is being followed.

Sociological reasons: Most of the cybercrimes remain unreported due to the hesitancy and shyness of the victim and her fear of defamation of family's name. Many times she considers that she herself is accountable for the crime done to her. The women are more

⁹¹ Supranote 3

vulnerable to the danger of cybercrime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Women fear that reporting the crime might make their family life difficult for them, they also question whether or not they will get the support of their family and friends and what the impression of society will be on knowing about them. Due to these fears women often fail to report the crimes, causing the spirits of culprits to get even higher.

Section 354A IPC - 'Sexual harassment' - A man committing any of the following acts- physical contact and advances involving unwelcome and explicit sexual overtures; or a demand or request for sexual favours; or showing pornography against the will of a woman; or making sexually coloured remarks, shall be guilty of the offence of sexual harassment. The first three offences of sexual harassment carry punishment of rigorous imprisonment for a term which may extend to three years, or with fine, or with both. The last offence of sexual harassment carries punishment of imprisonment of either description for a term which may extend to one year, or with fine, or with both.

Section 354D IPC- 'Stalking'- Any man who follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking. Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and shall also be liable to fine;

Section 354C IPC -'Voyeurism'- Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and shall be punished on a second or subsequent conviction, with imprisonment of either

description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine. "Private act" includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim's genitals, posterior or breasts are exposed or covered only in underwear, or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.

Where the victim consents to the capture of the images or any act but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section.

Women especially young girls inexperienced in cyber world, who have been newly introduced to the internet and fail to understand the vices of internet, and hence are most susceptible to falling into the bait of cyber criminals & bullies, Cybercrimes and cyber bullying is of various types, some are:

1. **Cyber Harassment:** Cyber Harassment is characteristic repetitive behaviour intended to disturb or up rest a person though use of internet. A particular class of harassment which is sexual in nature is known as sexual harassment, among several other things it majorly includes persistent and unwanted sexual advancement. Under Indian law sexual harassment has newly been defined under the Criminal Law Amendment (Bill) 2013 as physical contact and advances involving unwelcome and explicit sexual overtures; or

- (i) a demand or request for sexual favours; or
- (ii) making sexually coloured remarks; or
- (iii) forcibly showing pornography; or
- (iv) any other unwelcome physical, verbal or non-verbal conduct of sexual nature.

67 A, 67 B of the IT act provide sexual harassment in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, in the cyber world harassment including blackmailing, threatening, bullying, and even cheating is often done through e-mailing. Email harassment is very similar to harassing through letters; however, it is greatly difficult to crackdown upon

the culprits of crime in cyber harassment as often people create fake identities on internet for such purposes. ⁹²

2. Cyber stalking: Cyber Stalking basically is behavior wherein an individual willfully and repeatedly engages in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, torments, or terrorizes that person. This is one of the most talked about internet crimes in the modern world. Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites and email.

The motivation of stalkers may be considered less than four reasons,

- (i) sexual harassment,
- (ii) obsession for love,
- (iii) revenge and hate,
- (iv) ego and power trips..

Ritu Kohli Case

Ritu Kohli Case was India's first case of cyber stalking, in this case Mrs. Ritu Kohli complained to police against a person, who was using her identity to chat over the Internet at the website <http://www.micro.com/>, mostly in Delhi channel for four consecutive days. Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was also deliberately giving her phone number to other chatters encouraging them to call Ritu Kohli at odd hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on odd hours. The said call created a havoc in personal life of the complainant consequently IP addresses was traced and police investigated the entire

⁹² Debarati Halder, Cyber Crime against Women in India, CyberLawTimes.com, 25:10:2018, 05:00 PM, <http://www.cyberlawtimes.com/articles/103.html>

matter and ultimately arrested the offender. A case was registered under the section 509, of IPC and thereafter he was released on bail. This is first time when a case of cyber stalking was reported.

Similar to the case of email harassment, Cyber stalking is not covered by the existing cyber laws in India. It is covered only under the ambit of Section 72 of the IT Act that perpetrator can be booked remotely for breach of confidentiality and privacy. The accused may also be booked under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again for outraging the modesty of women.⁹³

Punishment for violation of Privacy (Section 66E) – 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. Offence is cognizable and bailable. Case is triable by the court of Magistrate of first class.

3. Cyber pornography: It refers to portrayal of sexual material on the web. This is the threat to the female netizens as they never know which actions of theirs are being recorded and would later end up on internet.

The DPS MMS scandal is a very famous case of this where an MMS clip of a school girl in compromising situation was made and distributed amongst various internet networks.

In another incident, at Mumbai, a Swiss couple gathered slum children and then forced them to appear for obscene photographs, which they took and then uploaded those photographs to websites specially designed for paedophiles. The Mumbai police arrested the couples for pornography .

⁹³ Supranote 5

The most recent example is of Delhi Metro CCTV footage leaks case, where the CCTV recording couples getting intimate in metro stations etc. which has been recorded by police security cameras has been leaked on internet.

Unlike other crimes like Cyber Stalking, Cyber Defamation, Morphing, Email Spoofing, Cyber Pornography is considered an exceptional case which has been covered by the IT Act 2000 to a certain extent by Section 67 of the IT Act 2000. Along with IT Act the perpetrator can be punished under various Sections of IPC (Section 290 for committing public nuisance, section 292 for sale of obscene books etc, and section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, section 293 for sale etc of obscene objects to young persons and then section 294 for doing or composing, writing etc of obscene songs and finally under section 509 for outraging the modesty of women).

Punishment for publishing or transmitting obscene material in electronic form (Section 67): Imprisonment for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second attempt or subsequent conviction with imprisonment of either description of a term which might be extend upto five years and also with fine which may extend up to ten lakh rupees. Offence is cognizable and bailable for the first conviction and non-bailable for the second conviction. Case is triable by the court of Magistrate of first class.⁹⁴

Punishment for publishing or transmitting obscene material in electronic form (Section 67A): Imprisonment for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second attempt or subsequent conviction with imprisonment of either description for a term which might be extend up to seven years and also with fine which may extend up to ten lakh rupees. Offence is cognizable and non-bailable. Case is triable by the court of Magistrate of first class.⁹⁵

⁹⁴ Akash Kamal Mishra, XVI Penalties and Offences under the IT Act, 2000 (Ed. 1 Ms. Avantika Johari, 2018)

⁹⁵ *Ibid*

Punishment for publishing or transmitting depicting children in sexually explicit act, etc., in electronic form (Section 67B): Imprisonment for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second attempt or subsequent conviction with imprisonment of either description for a term which might extend up to seven years and also with fine which may extend up to ten lakh rupees. Offence is cognizable and non-bailable. Case is triable by the court of Magistrate of first class. ⁹⁶

4. **Cyber defamation:** Cyber tort including libel and defamation is another common crime against women in the net. This occurs when defamation takes place with the help of computers and or the Internet.

The very first instance of cyber defamation in India was recorded in the case of SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra-Jogesh Kwatra - cyber defamation was reported when a company's employee (defendant) started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the plaintiff company. The plaintiff was able to identify the defendant with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

Another famous case involving a women was The State of Tamil Nadu Vs Suhas Katti - The case is related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. ⁹⁷

5. **Morphing:** Morphing is editing the original picture so as to make it look completely or largely different. Often criminally minded elements of the cyber world download

⁹⁶ *Ibid*

⁹⁷ Supranote 5

pictures of girls from websites such as Facebook and then morph it with another picture in compromising situation so as to represent that those women were indulging in such acts. Often the next step after this is to blackmail those women through the threat of releasing the morphed images and diminishing the status of those women in society. The recent Air Force Balbharati School case (Delhi) is a recent case comes under this category where a student of the School was teased by all his classmates for having a pockmarked face. He, who is tired of the cruel jokes, decided to get back at his tormentors and scanned photograph of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. The father of one of the class girls featured on the website came to know about this and lodged a complaint with the police.

Such acts can be penalised under I.T. Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC sec 509 also.

6. Email Spoofing : E-mail spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source; it is done by properties of the email, such as the From, Return-Path and Reply-To fields, ill-intentioned users can make the email appear to be from someone other than the actual sender. This method is often used by cyber criminals to extract personal information and private images from unsuspecting women, these images etc. are then used to blackmail those women. The most popular case of cyber spoofing is Gujrat Ambuja's Executive Case and blackmailing the Abu Dhabi based NRI.⁹⁸

Remedies:

1) The increasing number of crimes against women are a huge concern for any state however, cybercrimes make it even more challenging as criminals have the opportunity to create fake identities and then after indulge in illegal activities. To counter this government should make stricter laws to apply on the Internet Service Providers(ISP), as they alone have the complete record of all the data being accessed by anyone surfing

⁹⁸ Supranote 5

on net. ISPs should be made to report any suspicious activities that any individual is indulging into, this will help to curb crimes in nascent stage.

2) Legislation needs to make stricter regulation for cyber cafes, who should keep a record of their customers who utilized their internet services, often people go to cyber cafes to indulge in criminal activities so as their own IP addresses are not revealed in any future investigation. This is another manner to mask identity.

3) People need to be cautious over which parts of their daily lives are being recorded by cameras & should act modest in such times. Awareness over cyber culture and its back draws also need to be improved amongst people. People need to be made aware of their rights, studies show that a large population of internet users in India have no knowledge of their rights in such matters :

4) Email spoofing is possible because of Simple Mail Transfer Protocol (SMTP), the main protocol used in sending email, does not allow an authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, however this precaution is not always taken.⁵ So women should take precaution and always add the SMTP service extension with the SMTP client.

Unfortunately even today the Indian police tends to not tends to take cybercrimes seriously, in such scenario, the woman or the young girl who falls prey to cyber victimization should first contact a women assistance cell or NGO (such as All India Women's Conference , Sakshi , Navjyoti , Centre for cyber victims counselling) which will assist and guide them through the process, also this will make sure that police does not take any case lightly.

Conclusion

Women are safe neither in a physical World nor in virtual place like social networking sites. Crimes like online stalking, online defamation, pornography, voyeurism, cyber-harassment etc., are committed against women. IPC sections 354A, 354D, 354C and IT Act 2000 covers sections like 66A for sending offensive messages, 66E for violation of privacy, 67 for publishing obscene materials, 67A for transmitting obscene materials in electronic form, 67B for publishing children in sexually explicit act, exist to save the modesty of women from outraging.

More serious action is needed by the government side to save the women from growing offences committed against them.

