International Journal of Research in Social Sciences
Vol. 8 Issue 12, December 2018,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

THE REALITY OF VIRTUAL THREATS AGAINST WOMEN IN INDIA

Dr.BinduDogra[*]

Ms.ReevaKalra*

Abstract

Of the myriad information technology advancements, the Internet remains the most popular one. It is our one-stop-shop for all the information and it facilitates communication at a very fast speed, all over the globe. However, like there are two facets to a coin, similarly, the Internet, apart from all its advancements, allows crime to widen its roots in all directions. Cybercrime is a global phenomenon which hampers the privacy and security of a person online. Women are often the soft targets. Women especially young girls, inexperienced in cyber world, who have been newly introduced to the internet fail to understand the vices of internet, and hence are most susceptible to falling into the bait of cyber criminals (Misra, 2013). Though crime against women is on a rise in all fields, being a victim of cybercrime could be most traumatic experience for a woman especially in India where the society looks down upon the women, and the law doesn't even properly recognise cybercrimes. The present paper aims at discussing the various types of cybercrimes that can be inflicted upon a woman, how

Keywords:

Cyber defamation

Email spoofing

Morphing

Cyber bullying

[*] **Assistant Professor, Post Graduate Department of Sociology, MCM, DAV College for women, sec - 36, Chandigarh (UT), India.**

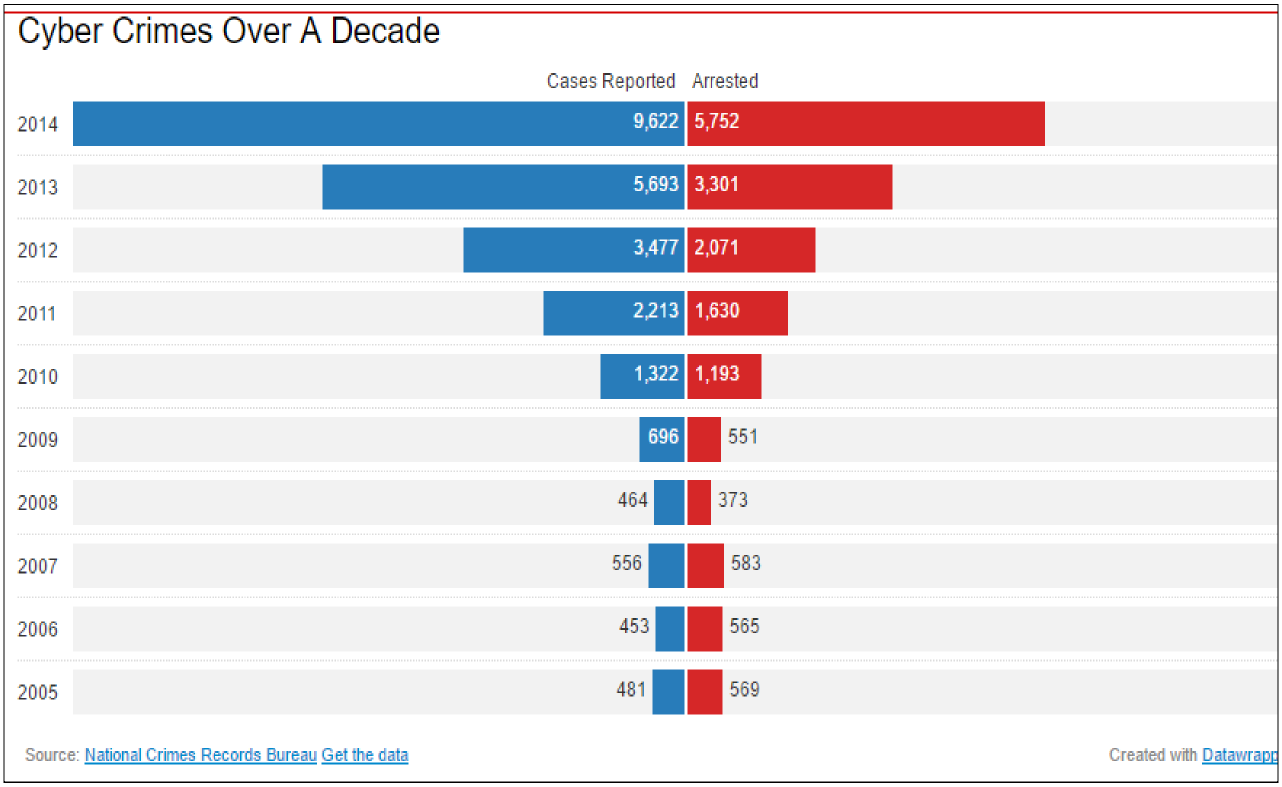
they adversely affect her and to ascertain the reasons for the growth of such victimization. It also briefly examines some of the famous cybercrime cases of India and laws that exist to protect women against cyber-crime and at the end are some suggestions to tackle these crimes.

Introduction

Of the myriad information technology advancements, the internet remains the most popular one. It is our one-stop-shop for all the information and it facilitates communication at a very fast speed, all over the globe. However, like there are two facets to a coin, similarly, the Internet, apart from all its advancements, allows crime to widen its roots in all directions. Cybercrime is a global phenomenon which hampers the privacy and security of a person online. Cyber-crime or computer crime is considered to be any crime that uses a computer and a computer network (Matthews, 2010). It is for unauthorized access or theft of stored or on-line data that can be used for several criminal activities against a victim. Therefore, Cybercrime refers to all the activities done with criminal intent in cyberspace. Today, there are many disturbing things happening in cyberspace.With the advent of technology, cyber-crime and victimization of women are on the high and it poses a major threat to the security of a person as a whole(Chauhan, 2012).

According to National Crimes Record Bureau, Cybercrimes reported in India rose 19 times over the last ten years, (2005 to 2014), it was 481 in 2005 and reached 9266 in 2014.These crimes were reported under IT Act, 2000.(Refer Table No. 1).

Table No. 1 Cybercrimes reported in India over the last ten years: from 2005 to 2014



Cyber Crimes Over A Decade

Source: National Crimes Records Bureau Get the data

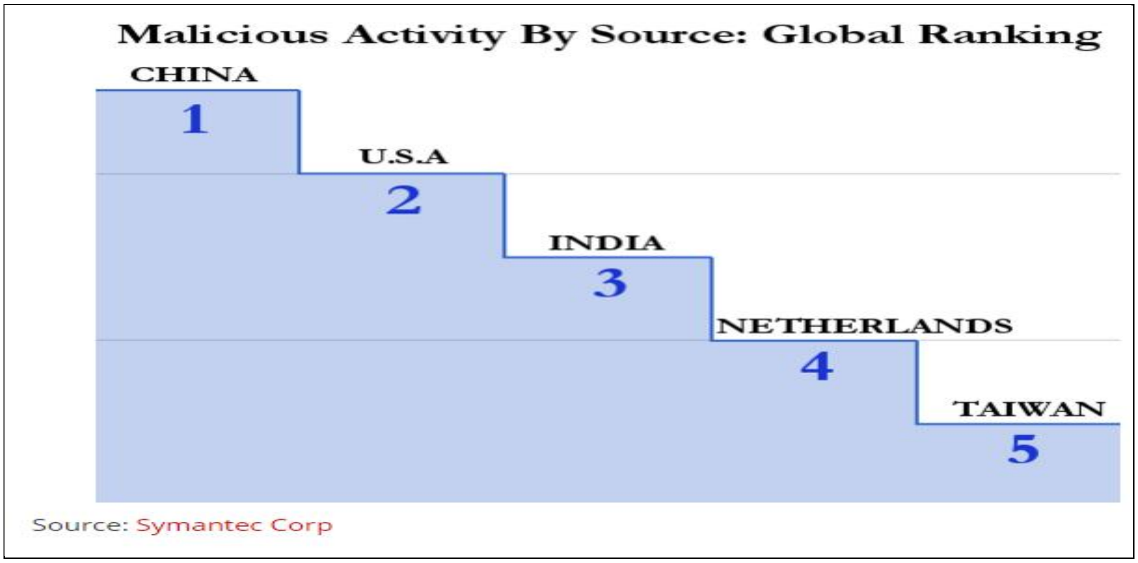
Created with Datawrapp

* Assistant Professor, Post Graduate Department of Sociology, MCM DAV, College, CHD.

** Post Graduate student of Sociology, MCM DAV, College, CHD.kalrareeva@gmail.com

It is shocking that India was ranked third worldwide, next to US and China, as a source of malicious activity in 2015, according to 2016 report by Symantec Corp, a software security firm (refer table No. 2). According to National Crimes Record Bureau, among Indian states Maharashtra reported the most cybercrimes (1,879) in 2014, followed by Uttar Pradesh, Karnataka, Telangana and Rajasthan. The top five states accounted for 63% of all cybercrime cases in India.

Table No. 2. Malicious activity Global Ranking by Symantec Corporation (Year 2015)



Source: Symantec Corp

Types of cybercrime against women

Women are often the soft targets in the cybernetic world. Women especially young girls, inexperienced in cyber world, who have been newly introduced to the internet fail to understand the vices of internet, and hence are most susceptible to falling into the bait of cyber criminals (Misra, 2013). Though crime against women is on a rise in all fields, being a victim of cybercrime could be most traumatic experience for a woman especially in India where the society looks down upon the women, and the law doesn't even properly recognise cybercrimes. Various types of cybercrimes women facing are:

- Cyber stalking - The University of Virginia defines cyber stalking as a behaviour wherein perpetrator wilfully and repeatedly engages in a knowing course of harassment directed at another person which seriously alarms, torments, or terrorizes that person. It involves invading the privacy by following a person's movements across the Internet by posting messages on the online bulletin boards, entering the chat-rooms frequented by the victim and constantly bombarding the victim with messages and emails with obscene language (Aggarwal&Kaushik, 2012). There are four reasons behind cyber stalking namely, for sexual harassment, for revenge and hate, for obsession love, and for ego and power trips (Jeet, 2012). It is believed that Over 75% of the victims of cyber stalking are female (Halder&Jaishankar, 2010)
- Cyber defamation - Cyber violence which includes libel and defamation is another common online crime against women. It occurs when someone posts defamatory matter about someone on website or sends emails containing defamatory information to person's friends (Agarwal&Kaushik2014). The harm through defamatory statements about any person on a

website is widespread and irreparable, as the information is available to the entire world which affects the victim as a whole (helplinelaw.com).

- Email spoofing - It is sending email to another person in such a way that it seems that the email was sent by someone else. It has become so common that we can no longer take for granted that the email one is receiving is truly from the person identified as the sender. These things happen in every city but only one in every 500 cases is reported (Halder&Jaishankar, 2008)
- Cyber pornography -It is the most dangerous threat to the female netizens. This would include pornographic websites or pornographic magazines produced using computers to publish and print the material and the internet to download and transmit pornographic pictures, photos, writings etc. Today, almost 50% of the websites contain pornographic material on the internet. This turns dangerous to a women's integrity as cyber criminals use photos of women and fix them with nude photographs or videos and the photograph or video resembles of that woman. (Halder&Jaishankar, 2011b).
- Morphing -Morphing is editing the original picture so as to make it look completely different. Often criminally minded elements of the cyber world download 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. This amounts to violation of I.T. Act, 2000 and attracts sec. 43 & 66 of this Act. The violator can also be booked under IPC (Yazdani, 2014).
- Cyber bullying -Cyber bullying is wilful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature (Hinduja&Patchin, n.d.). Globally, India is third behind China and Singapore in cyber bullying (Simhan, 2012).
- Cyber Hacking - Unauthorized access to one's data, profile, personal information, passwords or any such online activity is known as hacking. Criminals can change passwords or use this personal information for morphing or defamation.

The Impact of the above mentioned types of cybercrime on women can cause social, physical, mental, economic and psychological repercussions like depression, low self-esteem, agoraphobia, insomnia, post-traumatic stress disorder etc. Cyber defamation also leads to social defamation of the victim and her family(Gupta, 2017). Society often boycotts such women as they are considered social stigma and in extreme situations, victims often take extreme step of committing a suicide. Crimes in the virtual world at times lead to crimes in the real world: After receiving the personal information of the victim, the miscreant can use this information against the woman for causing harm, and it is one of the prime reasons for causing some of the heinous crimes like rape, murder, kidnapping of the victim. It also adversely effects on the career and economic status of the victim. Sufferers often lose their job due to insult they face in the society and workplace which poorly affects their life.

Keeping in mind such irremediable consequences, it is imperative to discuss the reasons for the growth of these cybercrimes. Some of the prominent reasons are:

- Cybercrime has become a profession- people involved in it have entered into the organised world of crime. They are associated with drug-trafficking, extortion and moneylaundering.It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. Various cybercrimes like pornography, morphing etc. have become commercial activities over internet and bring financial gains for the offenders and therefore are on an upward trend.
- Socio-cultural reasons - Nurturing practices in the Indian families as well as patriarchal system of Indian society are the major reasons why females become victims and are not very open about their victimization. They also doubt whether or not they will get the support of their family and friends and what the impression of society will be on knowing about the issue. It is the woman’s vulnerability that gives the power to the miscreant(s) for abusing her (Halder&Jaishankar, 2008).
- Victim’s fear of reporting crime - Out of the fear of causing harm to her family’s honour, she shies away from going to the police station, causing the spirits of culprits to get even higher. A woman abstains from complaining even if she is mistreated because once the crime is reported it is flashed through media or internet, and then it becomes more difficult for the woman to live in the society (Halder&Jaishankar, 2011a).
- Satisfaction of voyeuristic fantasies of perpetrators - Some criminals find women as objects of voyeuristic pleasure and indulge in such criminal activities for satisfaction of their sexual fantasies. There are some people who do it for adventure to get insights of the crimes

taking place over cyber space but with time these amateurs become experts in cybercrime, further increasing victimization of women.

- Partial computer knowledge - Some Women have partial knowledge in using this technology and they mainly use computer and internet as an instrument for gathering knowledge. They are also unknown about privacy protection which helps criminals to steal their personal data easily.
- Lack of awareness about cyber laws and anonymity of miscreants - Some laws have been designed for email spoofing, cybersex, trespassing into others' privacy etc. However, the laws related to cybercrime against women are correlated to sexual crime and abuses on the internet, but there are many practical difficulties associated with punishing the miscreant. Primarily, many women are not aware of the laws against cybercrime (Halder&Jaishankar, 2008). And also the cyber world is a virtual space where it becomes very easy for the perpetrator to manipulate his identity and hide. This also results in increase of cybercrime against women as the miscreant(s) goes scot free (Saha&Srivastava, 2014).
- Changing lifestyles of women - With fast changing life styles and loneliness women fall prey to social networking sites. They make accounts and profiles on these websites and start making friends. They tend to spend more time online without being aware of pitfalls of the cyber space. This makes them more vulnerable to targeted online attacks.
- Inadequate cyber forensic labs and cyber forensic experts- The police do not know how to conduct a proper search in a computerised environment, particularly in a networked ecosystem. Most of the times, the police is also not aware of the correct tool or software that needs to be used to collect evidence especially when the identity of the culprit is unknown.There are not many cyber forensic experts in the country and cyber forensic labs are also inadequate. Therefore, they lose out on vital evidence and clues. This leads to acquittal of criminals (Lahiri, 2014).

Following are some well-known cybercrime cases which were discussed by media at length; they were examined in the present paper for comprehensive understanding of modes operandi adopted by the perpetrators to harm their victims:

- **RituKohli Case** –this was India's first case of cyber stalking. In this case Mrs.RituKohli 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. She 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 RituKohli at odd hours. Police investigated the entire matter and ultimately arrested the offender. The case was registered under the section 509, of IPC but sadly thereafter the perpetrator was released on bail. This is first time when a case of cyber stalking was reported (Jeet, 2012).

- **Mumbai 2011 child pornography case** – the second case examined took place in Mumbai in 2011, 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(someone who is sexually interested in children). The Mumbai police arrested the couple for pornography (Rathinasabapathy&Rajendran, 2007).
- **Net pornography incident at BalBharti School-** A 16-year-old boy was arrested in April 2001 on the charge of creating a pornographic website containing obscene comments about some women teachers and girls of his school, in Delhi. When he was released on bail, the school refused to take him back.
- **SuhasKatti v. Tamil Nadu case-** it was the first case in India where a conviction was handed down in connection with the posting of obscene messages on the internet under the section 67 of the Information Technology Act, 2000. The case was filed in February 2004 and in a short span of about seven months from the filing of the FIR, the Chennai Cyber Crime Cell achieved the conviction. In the case, a woman complained to the police about a man who was sending her obscene, defamatory and annoying messages on a Yahoo message group. The accused also forwarded emails received in a fake account opened by him in the victim's name. The victim also received phone calls by people who believed she was soliciting (http://www.cyberralegalservices.com).

Some suggestions to tackle cyber crimes

Some of the Legal safeguards which are available in this domain are:

- IT Act 2000: It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India(Gandhi,n.d.).

- The Indecent Representation of Women (Prohibition) Act, 1986 is an Act of the Parliament of India which was enacted to prohibit indecent representation of women through advertisement or in publications, writings, paintings, figures or in any other manner. (http://wcd.nic.in/act/indecent-representation-women).

Besides, depending on legal system against cybercrimes, the need of the hour is that women have to be aware of cyber victimization by self. Today, every netizen wants to browse web privately and safely especially women, so it's important to follow some safeguards. Here are some steps and suggestions that women can follow and save themselves of being victims in cyber space and can make their online perceptions and experiences a safer one (Singh, 2015). Some suggestions and steps to tackle cyber-crimes are:

- Never reveal your home address. This rule is especially important for women who are business professionals and very visible. You can use your work address or rent a private mailbox. Just don't have your home address readily available(Moore,2018)
- Password protect all accounts including cell phones, land lines, e-mails, banking and credit cards with a secure password that would be difficult for anyone to guess. Change it every year. Your secret questions should not be easily answered either (Moore,2018)
- Conduct an internet search using your name and phone number. Be sure that there is nothing out there that you are not aware of. A cyber stalker may have created a craigslist account, web page or blog about you. Only you can stay on top of how your name is being used online(Moore,2018)
- Maintain stable social relationships: It is also the fact that we all like to believe that we should have 2000 Facebook friends. Probably, we don't need those 2000 Facebook friends, because we are unable to really know more than 150 of them. Maintaining a limit on the number of the people will ensure our information is distributed to people who you really know (Pennelli, 2012).
- Awareness campaign against cybercrimes: Awareness campaign must be set up from the grass root level such as schools, colleges etc. about cybercrimes like stalking cheatings, defamatory activities, misusing emails and social networking websites, virtual rapes, cyber

pornography, email spoofing etc. (Halder and Jaishankar, 2010). These campaigns can be beneficial in paralyzing cybercrimes.

- Seminars and workshops for better understanding of cyber victimization: Police, lawyers, social workers, and NGOs must be invited to education institutes, clubs, corporate offices, awareness-campaigns, seminars and workshops to discuss about legalities and illegalities of cyber conduct among adults inclusive of both genders. Reporting of cyber victimization at all levels directly to the police and NGOs working cybercrimes must be encouraged. Secondly, workshops and seminars must be conducted for the police personnel for better understanding of such kinds of victimization and quick responses towards the complaints(Halder&Jaishankar, 2010).
- Rigid and stringent laws: India must bring in more rigid and stringent laws for cybercrimes against women in the cyber space. It is evident that present India's Information Technology Act includes only few sections for cybercrime, especially against women, hence to curb cybercrimes, either IT Act must be re-modified or separate law on cybercrimes should be created.Proper law and order against crimes may lead to create better society.
- Beware of unsolicited calls and messages: Woman should avoid unwanted or unsolicited phone calls and messages because cell phone may be monitored. If it happens again and again, you should try to record phone calls of harasser and report to the police (Halder and Jaishankar, 2010). Even, they should download applications from trusted websites. Besides, they should discuss and share the problem regarding cyber harassing with their trusted ones like parents, mates or spouses etc.(Singh,2015).
- Understand privacy settings of social network: Social networks and other online content and service providers all have privacy policies and private settings. One must try to understand privacy policies and adopt privacy settings that help in protecting oneself from any potential risk or online harm. So, we must have the knowledge about privacy settings of social networking (Pennelli,2012).
- Check account regularly: It is clear that every net user has its own account on network sites. We should regularly check our email, blog or website accounts. By doing so, we will be in-touch with our belonging accounts on internet and we can lessen the possibilities of hacking, stalking etc. by reviewing our account. It is found that some women don't check their account after they make their accounts on internet(Moore,2009).

- Protect data on the move: In our daily life, we often use public computers in internet cafes etc. You should remember that when you are using internet on public computers, web browsers can keep a record of your passwords and every page you have visited. So, you should not forget to erase your tracks or history on web browsers (Doyle, 2012). In other words, women should be distrustful in nature while using internet because stalker may try to rip you off (Singh, 2015).
- Seeking help from women assistance cells and NGOs: Unfortunately, even today the Indian police tends to not 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, Saakshi, 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 - There is no denying of the fact that the impact of internet usage has been both positive and negative. On the one side it has helped individuals in better decision making, improved livelihood, entertainment, easy and affordable learning, development of e- commerce etc., and on the other side it has also given birth to crime in the cybernetic world. The association between internet users and cybercrime cases is significant. All over the world the usage of internet is ever increasing therefore the incidence of cybercrime is inevitable. Women being soft-hearted tend to trust others easily; this makes them more vulnerable to cybercrime. But also people have to change their mind-sets towards women and should develop the sense of commonality and not to consider woman as a commodity. The need of the hour is that by taking various preventive measures we can reduce the increasing incidence of cybercrime against women.

References:

- Agarwal, N., &Kaushik, N. (2014). Cybercrimes against women. *GJRIM,4*(1), 37-49.
- Chauhan, M. (2012). Preventing cybercrime: A study regarding awareness of cybercrime in tricity. *International Journal of Enterprise Computing and Business Systems,2*(1). Retrieved from http://www.ijecbs.com/January2012/35.pdf

- Cyber defamation in India. (n.d.). Retrieved from http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html
- Cybercrimes over a decade [Chart]. (n.d.). In *National Crime Records Bureau*. Retrieved from https://scroll.in/article/809244/as-internet-use-spreads-cyber-crimes-rise-19-times-over-10-years.
- Doyle, C. (2012, February 7). Top tips to avoid being a cybercrime victim. Retrieved August 27, 2018, from https://www.siliconrepublic.com/gear/top-tips-to-avoid-being-a-cyber-crime-victim
- Gandhi, B. (n.d.). *Indian Penal Code*. India: Eastern Book Company.
- Gupta, K. (2017, August 1). 10 essential online safety tips for women. Retrieved from shethepeople.tv https://www.shethepeople.tv/news/essential-online-safety-tips-women-cyber-crime
- Halder, D. (n.d.). Cybercrime against women in India. Retrieved from http://www.cyberlawtimes.com/articles/103.html
- Halder, D., &Jaishankar, K. (2008). Cybercrimes against women in India: Problems, perspectives and solutions. *TMC Academic Journal*, 3(1), 48-62.
- Halder, D., &Jaishankar, K. (2010). *Cyber victimization in India: A baseline survey report* (Rep.). Retrieved http://www.cybervictims.org/CCVCresearchreport2010.pdf
- Halder, D., &Jaishankar, K. (2011a). Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India. *Victims and Offenders*, 6(4), 386-398. doi: 10.1080/15564886.2011.607402.
- Halder, D., &Jaishankar, K. (2011b). *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, USA: IGI Global.
- Hinduja, S., &Patchin, J. W. (n.d.). *Cyberbullying Fact Sheet What you need to know about online aggression* (Rep.). Retrieved from https://cyberbullying.org/cyberbullying_fact_sheet.pdf
- Important Cyber Law Case Studies. (n.d.). Retrieved from http://www.cyberralegalservices.com/detail-casestudies.php
- India, Ministry of Women and Child Development. (n.d.). *Indecent Representation of Women*. Retrieved from http://wcd.nic.in/act/indecent-representation-women

- Jeet, S. (2012). Cybercrimes against women in India: Information Technology Act, 2000. *Elixir International Journal*. Retrieved from https://www.elixirpublishers.com/articles/1351168842_47 (2012) 8891-889
- Lahiri, A. (2014, May 13). "Cyber forensic facility in India is inadequate". Retrieved from https://www.governancenow.com/views/interview/cyber-forensic-facility-india-inadequate
- Malicious activity by source: Global ranking [Chart]. (n.d.). In *Symantec Corp*. Retrieved from https://scroll.in/article/809244/as-internet-use-spreads-cyber-crimes-rise-19-times-over-10-years.
- Matthews, B. (2010). Computer Crimes: Cybercrime Information, Facts and Resources. Retrieved from http://www.thefreeresource.com/computer-crimes-cybercrimeinformation-facts-and-resources
- Misra, Rajat, Cyber Crime Against Women (April 10, 2013). Retrieved from SSRN: https://ssrn.com/abstract=2486125
- Moore, Alexis A. (2009, January 8)12 Tips To Protect Yourself From Cyberstalking. Retrieved from http://womensissues.about.com/od/violenceagainstwomen/a/CyberPrevention.htm
- Moore, Alexis A. (2018, June 14). 12 Crucial Tips to Protect Yourself from Cyberstalking. Retrieved from https://www.thoughtco.com/tips-to-protect-yourself-from-cyberstalking-3534318
- Pennelli, P. (2012, January 31). Cyberstalking Awareness: Protect Yourself On-Campus and Beyond with These 7 Steps. Retrieved August 27, 2018, from https://blog.gradguard.com/2012/01/31/cyberstalking-awareness-protect-yourself-on-campus-and-beyond-with-these-7-steps/
- Rathinasabapathy G. & L. Rajendran. (2007).Cyber Crimes and Information Frauds: Emerging Challenges for LIS Professionals.*National Conference on Recent Advances in Information Science and Technology* (pp. 131-142). Madras Library Association & IGCAR, Kalpakkam.
- Saha, T., &Srivastava, A. (2014). Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization. *International Journal of Cyber Criminology*, *8*(1), 57-67.

- Simhan, T. R. (2012, June 26). India ranks third in cyber bullying. *The Hindu BusinessLine*. Retrieved from https://www.thehindubusinessline.com/info-tech/india-ranks-third-in-cyber-bullying/article20458143.ece1
- Singh, J. (2015). Violence against women in cyber world:A special reference to India. *International Journal of Advanced Research in Management and Social Sciences,4*(1).
- Yazdani, G. (2014). Cybercrimes against women in national and international perspective: Need for effective laws. *The Lex-Warrier: Online Law Journal,5*(11). Retrieved from http://www.lex-warrier.in/2014/11/crimes-against-women-in-cyber-space-internet-crimes/