# CYBER HARASSMENT AND VICTIMIZATION: COMPROMISING WOMEN'S PRIVACY[1]

## INTRODUCTION

"*I am not what happened to me, I am what I choose to become*"

- KARL JUNG

Internet has made it way easier to remain connected with our distant friends and relatives. Socialization through social networking websites (SNWs) has become a favorite hobby for "gizmo freaks", self supporting, educated, independent, modern women of the 21st century.[2]The advent of cyber world as a technology to enable easy, quick and feasible communication has also brought in big snags with it. Digitalization is the upshot of many innovations and technological advancements.[3] At one side of the coin the digitalization has enhanced the system of India in all terms such as economy, education, governance etc., but at second it brought cyber-crimes[4] also in India at large number. The internet also provides ground for illegal activities and makes many people exposed and vulnerable such as cybercrime and online sexual harassment.[5] Every second, one woman in India gets tricked to be a victim of cyber crimes and the online platform is now the new platform where a woman's dignity, privacy and security is increasingly being challenged every moment.[4] Online violence against women takes various forms of abuse and includes, but is not limited to, online misogyny, text-based abuse (e.g. on social media platforms such as Twitter or Facebook), up skirting, image-based sexual abuse (also referred to as 'revenge pornography'), rape pornography, doxing, cyberstalking and cyber-harassment.[5]

But under Indian law "Cybercrime" as such has not been defined under any legislation. One legislation that deals with the offences related to such crimes in India is Information Technology Act, 2000, which was also further amended in the form of IT Amendment Act, 2008.[6]

Indian women are not able to report cyber crimes often as they are not really aware as to where to report such crimes or are afraid about reporting the same because of social embarrassment they have

---

[1] Disha Mohanty & Sherya Dalmia, Amity University Chhattisgarh, Raipur.

[2] Debarati HalDer, Karuppannan JaisHanKar; Cyber Socializing and Victimization of Women; September 2009 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.430.6685&rep=rep1&type=pdf

[3] Shweta Sankhwar, Arvind Chaturvedi; WOMAN HARASSMENT IN DIGITAL SPACE IN INDIA; 2018 https://acadpubl.eu/hub/2018-118-21/articles/21b/68.pdf

[4] Dhruti M Kapadia;Cyber Crimes Against Women And Laws In India; 21st November 2018: https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/

[5] Dr Kim Barker,Dr Olga Jurasz; Submission of Evidence on Online Violence Against Women; November 2017; https://dspace.stir.ac.uk/bitstream/1893/26282/1/Barker_Jurasz%20UN%20Submission%20on%20online%20violence%20against%20women_Nov%202017.pdf

[6] Cyber Crimes in India – an Introduction; March 25 2013;https://www.vakilno1.com/legalviews/cyber-crimes-in-india.html

to face. Most of the problems can be solved if women report the crime immediately and strict actions were taken against.[7]Thus, there is an urgent need of bringing awareness and consciousness among women to be careful while using internet facilities and also a proper guidance if somehow, they face cyber- crime then they can raise their voice against it.[8]

So this paper attempts to discuss different threats faced by women in cyber space, the reasons and various strategies to deal with the violence.

## PART II- PROBLEMS ASSOCIATED

It is a well known fact that with rapid development in every sphere, lifestyle of individual has witnessed a sea change. 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.[9]

Women especially young girls inexperienced in cyber world, who have been newly introduced to the internet fails to understand the consequence of revealing personal information be it for any reason i.e..for job requirement, matrimonial sites or any bank details becomes an easy target for the culprit. The miscreant uses this information against the women for causing harm in various ways:-

### 1) Cyber Stalking-

Cyber stalking a way to use the Internet to stalk someone for online harassment and online abuse. A cyber stalker does not engage in direct physical threat to a victim, but follows the victim's online activity to gather information, make threats in different forms of verbal intimidation. These types of stalking can occur via social media, e-mail, chat rooms, message boards and discussion forum. To be considered as cyber stalking, the acts must take place repeatedly and be perpetrated by the same person.

### 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 using her name to chat, giving out personal details and using obscene languages. The same person was purposely giving her phone number to other users

[7] *Ibid*
[8] *Ibid*
[9] Rajat Misra, Cyber Crime Against Women, (April 10);https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2486125

encouraging them to call Ritu Kohli at odd hours. As a result, Mrs. Kohli had received almost many calls 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 matter and ultimately arrested the offender. A case was registered under the section 509, of IPC but he was released on bail.[10]

**Vinu Priya Case**[11]

On June 23 the first photograph of the 21 year old victim appeared, she informed her parents who lodged a complaint with the Cyber Crime Cell. The police, either lacking the investigative skills to trace the origin of the morphed photograph or simply displaying lack of interest, told Vinupriya's father that it will nab the culprit in two weeks. One of the officers in the Cyber Crime Cell allegedly asked for bribe in form of a mobile phone if the father wanted the investigation to be done. Vinupriya's father says he bought a cell phone worth Rs 2,000 for the cop and bemoans that despite taking a bribe, the officer did not deliver justice. On June 26, another obscene photograph was posted on Facebook, leaving Vinupriya traumatized. The investigating officer had already pre-conceived that she must have sent those pictures and now they were being posted, perhaps by a jilted lover. On 27th june being alone at home, she killed herself. The second photograph that had appeared on June 26, disappeared within hours of news of Vinupriya's death becoming public.

Proof, that the pervert was lurking somewhere close by or was part of Vinupriya's friend circle.

**2) Cyber Pornography**-

Cyber Pornography is another threat to women and children because this includes publishing pornographic materials in pornography websites by using computers and internet. Today, almost 50% of the web sites are contained with pornographic material on the Internet. This turns dangerous to a woman'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 only.[12]

Cyber Pornography has also give rise to "Revenge Porn"[13]. In India, the offence is tried under provisions of the IT Act. While the relevant sections are effective and stringent, the fact remains that they do not account for the degree of violation as the prosecutor put it—virtual rape. The IT Act does not protect and support the victim in the way sexual assault and rape laws do.[14]

---

[10] Supra11

[11] Palanisamy v. State of Tamil Nadu

[12] Halder, D., & Jaishankar K. (June, 2011) Cyber-crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN: 978-1-60960- 830-9

[13] Non-consensual sharing of intimate sexual images by former partners.

[14] The New Indian Express,Dealing with 'revenge porn',16th March 2018; http://www.newindianexpress.com/opinions/editorials/2018/mar/16/dealing-with-revenge-porn-1787897.html [18] (2005) 3 CompLJ 364 Del

**Avnish Bajaj v State**[18]

The case involved an IIT Kharagpur student Ravi Raj, who placed on the baazee.com a listing offering an obscene MMS video clip for sale with the username alice-elec. Despite the fact that baazee.comhave a filter for posting of objectionable content, the listing nevertheless took place with the description, "Item 27877408 – DPS Girls having fun!!! full video + Baazee points." The item was listed online around 8.30 pm in the evening of November 27th 2004 and was deactivated, around 10 am on 29th November 2004. The Crime Branch of Delhi police took a step forward in the matter and lodged an FIR. Upon investigation, a charge sheet was filed showing Ravi Raj, Avnish Bajaj, the owner of the website and Sharat Digumarti, the person responsible for handling the content, as accused. Since, Ravi Raj absconded; the petition was filed by Avnish Bajaj, seeking the quashing of the criminal proceedings.

The court observed that there is a prima facie case for the offence under Section 292 (2) (a) and 292 (2) (d) IPC both in respect of the listing and the video clip respectively. The court observed that "by not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene", and thus it held that as per the strict liability imposed by Section 292, knowledge of the listing can be imputed to the company.

**3) Cyber Defamation-**

Cyber defamation includes both libel and defamation. It involves publishing defamatory information about the person on a website or circulating it among the social and friend's circle of victims or organization which is an easy method to ruin a woman's reputation by causing her grievous mental agony and pain.[15]It is mostly committed by hacking someone's id on FaceBook, Google, or any other social networking or mailing website. It is also done by creating fake profile of a person containing all personal information about that person, which resembles to be a genuine one to others on any website.[16]

[15] Supra6

[16] Dr. Monika Jain,VICTIMIZATION OF WOMEN BENEATH CYBERSPACE IN INDIAN UPBRINGING,April – June, 2017, http://docs.manupatra.in/newsline/articles/Upload/786274E9-B397-4610-8912-28D6D03230F9.monika_jain_pdf_11111.pdf

**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 post resulted very badly as the lady started getting annoying phone calls in the belief that she was soliciting.

**4) Photo Morphing-**

Editing of the original picture by unauthorized user or fake identity is termed as Morphing. It was identified that female's pictures are downloaded by fake users and again re-posted/uploaded on different websites by creating fake profiles after editing it.[17]

The photographs of the female are taken and they are morphed for pornographic purposes by using different parts of the pictures, for instance, the head or up to breast. Perpetrators due to internet access can in few seconds download women's pictures from social media, WhatsApp or some other resources and upload morphed photos on other websites such as social media site, porn sites or for registering themselves anonymously.[18]

**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. The boy being tired of the cruel jokes, decided to get back at them and scanned photograph and morphed them with nude photographs and uploaded in the free website. The father of one of his classmate (girl) featured on the website found it and lodged a complaint with the police.[19]

## PART III- WHY CYBERCRIME?

Most of the cyber crimes remain unreported due to the hesitation and shyness of the victim and her fear of defamation of family's name. Most of the times a girl believe that she herself is responsible for the crime done to her. The women are more susceptible to the danger of cyber crime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Women tend not to complain against sexual harassment, whether

[17] Ibid
[18] Supra6
[19] Supra11

they suffer it in real world or the virtual world they prefer to stay low and back off the matter as they feel that it may disturb their family life.[20]

It is a very expensive and time consuming process not to mention emotionally draining. Also, most crimes go unreported because women either fear or feel embarrassed to report their case to the police on account of social embarrassment. Humiliation, mental torture, stress, depression aggravates the situation.[21]

**Legal reason**

The main reason for the increased number of cyber-crimes against women in India is mainly due to lack of legal security. The State and law enforcement authorities are accountable to take productive measures to curb cyber sexual harassment. Stringent laws and implementation procedures need to be introduced. Time demand female cyber cells, female judges and female cops to deal with the situation as they themselves can understand the gravity of situation better. On account of delayed justice, people have lost faith in the law enforcement authorities. Lack of legal awareness makes it more complex. Further, most women do not even check the privacy rules and regulations listed on the social networking websites before joining into it. In fact, women can help regulate cyber obscenity by becoming vigilant about their rights and by ensuring safety measures prescribed by the various social networking websites. Most of the popular websites state their privacy policies declaring they will not take any responsibility for any sort of harassment caused to the users by other users. Websites also provide for safety options on menu bar of the culprit and warning them of their behavior and deleting their accounts. Therefore, women should only register after reading up the privacy policies. In most cases, negligence serves as a root cause for women being often trapped and victimized in incidents of cyber obscenity. Laws in India do not directly acknowledge many of the offences like cyber bullying, cyber eve teasing, cyber harassment, cloning of profile etc. in the Information Technology Act, 2000. The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty trying to address cyber crime by harmonizing national laws, improvising investigation techniques, and more cooperation among nations. However, is does not include any provisions pertaining to cyber

[20] Shobhna Jeet, Cyber crimes against women in India: Information Technology Act, 2000 ,12 June 2012 https://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf

[21] Yeshwant Naik, Cyber obscenity and victimisation of women in India, May 9, 2017 https://blog.ipleaders.in/cyber-obscenity/

obscenity in relation to women. Thus, generally the lack of uniform or universal laws, covenants and rules have boosted the growth of online women harassment.[22]

The object of the IT Act is crystal clear from its preamble which shows that it was created mainly for enhancing e- commerce hence it covers commercial or financial crimes i.e. hacking, fraud, and breach of confidentiality etc. but the drafters were unaware about the safety of net users. The most of the cyber crimes other than e- commerce related crime are being dealt with these three sections. Cyber defamation, cyber defamation, email spoofing, cyber sex, 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 provisions13. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for outraging the modesty of women is protected under Section 506 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences and prosecuted under IPC. The modesty of women seems not to be protected in general except for Section 67 which covers cyber sex in Toto.

As it has been discussed earlier that ineffeable nature of Internet is one of the main reasons for the growth of cyber crime so whereas Section 75 of the IT Act deals with the offences or women still do not go to the police to complain against sexual harassment, whether it is in the real world or the virtual world they prefer to shun off the matter as they feel that it may disturb their family life.[23]

**How privacy of a women is compromised?**

According to many conducted survey it is clear that, women are the ones who faces cyber harassment at the utmost level. The report suggests the cyber bullying faced by girl child in various countries. And India is leading the chart

| Rank | Country | 2018 | 2016 | 2011 |
|---|---|---|---|---|
| 1 | India | 37 | 32 | 32 |
| 2 | Brazil | 29 | 19 | 20 |
| 3 | United States | 26 | 34 | 15 |
| 4 | Belgium | 25 | 13 | 12 |
| 5 | South Africa | 26 | 25 | 10 |

[22] Ibid

[23] Supra22

Despite a mixed bag of regressive and progressive laws, the higher courts in India have made an effort to recognize the agency of women.

Whether it is autonomy to choose one's profession (women's right to work in dance-bars or make reproductive choices, as affirmed in the right to personal liberty guaranteed by Article 21 of the Constitution, the Supreme Court of India has at various instances affirmed women's right to privacy. However, it was only in August this year that the Supreme Court of India ruled that the right to privacy is indeed a constitutional right. The bench made a causal connect 'linking the three aspects of privacy (bodily integrity, informational privacy, and the privacy of choice) ... with the preamble of the Constitution, which guaranteed democracy, dignity, and fraternity'.The judgment also acknowledges the feminist critique that privacy – as in the private sphere – can act as veil for patriarchy to perpetuate violence. The court observed;

"The challenge in this area is to enable the state to take the violation of the dignity of women in the domestic sphere seriously while at the same time protecting the privacy entitlements of women grounded in the identity of gender and liberty."

This path breaking ruling, and hopefully, the new developments in the law, will pave the way for more progressive frameworks, rooted in furthering the privacy, dignity and agency of women, encouraging women to employ the law as a key instrument of their empowerment.

## PART IV- LEGISLATIVE RESPONSE

With the growing years, the crime rate all over the world is also increasing be it physically or virtually. With an omnipresent monster such as the internet that stands within the reach of as many as 3.58 billion users globally, it is very important for users to keep up with the amendments and new laws which would be helpful when in need.[24] Law does provide a remedy against most of the prevalent cyber crimes. The cyber crime is listed under The Information Technology Act, 2000 and was amended in the year 2008, due to the hike in crimes (omniform crimes). However, IT Act is not the only enactment covering cyber crime, the Indian Penal Code also initiates prosecution against cyber crime or to reinforce the provisions of IT Act.

[24] Amrtansh Arora, Ladies, here are 9 laws you should know about online stalking, harassment and obscenity, Timesnownew, Jan 5,2018, https://www.timesnownews.com/mirror-now/society/article/9-laws-you-should-knowabout-online-stalking-harassment-obscenity-cybercrime/185352

Under the Information and Technology Act, 2000, stalkers and cybercriminals can be booked under several sections for breaching of privacy:

**Section 66A**: Sending offensive messages through communication service, causing annoyance etc., through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment up to three years or fine.[25]

**Section 66E**: Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Three years of imprisonment or two lakhs rupees fine or both is the punishment provided for this.[26]

**Section 67**: It deals with publishing or transmitting obscene material in electronic form. The earlier section in ITA was later widened as per ITAA 2008 in which child pornography and retention of records by intermediaries were all included.[27]

**Section 72**: Punishment for breaching privacy and confidentiality.[28]

**Section 354A of the IPC:**

People posting lewd comments on social media are liable under this law and can be punished with one-year imprisonment and fine.

In addition, posting/messaging content related to pornography against the will of a woman or requesting sexual favours are punishable by a fine along with three years of imprisonment under the same provision.[29] **Section 354C of the IPC:**

This act deals with voyeurism which is a criminal offence under both the IPC and the IT Act. It deals with cases where a man, without the consent of a woman, captures an image/video of her engaged in a private act. Such an act is punishable by one to three years of imprisonment along with a fine.

[25] Supra6
[26] Ibid
[27] Supra3
[28] Ibid
[29] Supra 28

This provision can be referred to especially in cases when the woman does not expect to be observed by the accused.[30] **Section 354D of the IPC:**

This provision of the IPC deals with what is commonly referred to as "online stalking". The provision covers the grounds of a case where an attempt to contact a woman is made via the internet, email or any other form of electronic communication with the intention of establishing personal interaction despite her visible disinterest. Such an act is punishable with three years of imprisonment on the first count followed by five years of imprisonment on the second count both of which are in addition to a monetary fine.[31] **Section 499 of the IPC:**

Any individual who believes that his/her reputation is being harmed by a visible representation published on the internet can invoke this provision which exclusively accounts for remarks on social media or obscene images or videos posted for public consumption. Under this provision, defaming a woman online will land the perpetrator in jail for a period of two years.[32] **Section 503 of the IPC:**

In the case of an individual threatening a woman with the intention to either alarm her or malign her reputation, the former is liable to be penalised with a jail term of two years.[33] **Section 507 of the IPC:**

Under this provision, any individual who acts in the interest of intimidating or threatening a woman by anonymous communication is liable to be punished with two years in prison.[34] **Section 509 of the IPC:**

Under this provision, a person distinctly posting sexual remarks/pictures/videos comprising of sexual insinuations on social media is liable to three years of imprisonment along with a fine.[35]

## PART V- CAMPAIGN

### UNiTE to End Violence against Women

Launched in 2008, United Nations Secretary-General Ban Ki-moon's UNiTE to End Violence against Women campaign is a multi-year effort aimed at preventing and eliminating violence against women and girls around the world.

[30] Ibid
[31] Ibid
[32] Ibid
[33] Ibid
[34] Ibid
[35] Ibid

UNiTE calls on governments, civil society, women's organizations, young people, the private sector, the media and the entire UN system to join forces in addressing the global pandemic of violence against women and girls.[36]

The campaign was based on existing international legal and policy frameworks, and works to speed up the efforts of all UN offices and agencies putting effort into ending violence against women.

**The 16 Days Of Activism**

The 16 Days of Activism Against Gender-based Violence is a global campaign and was started in 1991.The campaign hopes and try to raise awareness about gender-based violence as a human rights issue at the all level. The 16 days of Activism spanning from International Day for the Elimination of Violence against Women on 25 November, through Human Rights Day on 10 December, has became an annual campaign against gender-based violence.[37]

In the streets, in schools, offices, villages and cities, every year, people around the world galvanize to raise awareness and take action during the 16 Days of Activism against Gender-Based Violence. For far too long, impunity, silence and stigma have allowed violence against women to escalate to pandemic proportions—one in three women worldwide experience gender-based violence.

The time for change is here and now women should be themselves responsible to take safety measures.[38]

In recent years, the voices of survivors and activists, through campaigns such as #MeToo, #TimesUp, #Niunamenos, #NotOneMore, #BalanceTonPorc and others, have reached a crescendo that cannot be silenced any more.

This is why the UNiTE Campaign's global advocacy theme this year is: Orange the World: #HearMeToo

[36] UNWOMEN, UNiTE to End Violence against Women, http://www.unwomen.org/en/what-we-do/ending-violenceagainst-women/take-action/unite

[37] UNWOMEN,16 ways, 16 Days: Your guide to ending violence against women, November 21, 2018, http://www.unwomen.org/en/news/stories/2018/11/feature-guide-to-ending-violence-against-women

[38] UNWOMEN, 16 days of activism, http://www.unwomen.org/en/what-we-do/ending-violence-against-women/takeaction/16-days-of-activism

**Digital Hifazat**

In 2016, we launched the #DigitalHifazat campaign alongside our research report that showed how women are subjected to online violence during these 16 Days of Activism as well.

Based on the findings of our research report, we advocated for a safe and secure internet for all using articles and videos to illustrate the rampant nature of online violence against women.

In 2017, we expanded this campaign to take a broader look at the ways in which women experience the internet – both good and bad. The internet can be a space of violence, but also one of empowerment. We looked at ways in which women use the internet to fight back against oppressive systems of power that seek to limit their voice and expression.

Furthermore, oppression is intersectional, and we hoped to display how different communities of women in India experience the internet – their struggles, their victories, how it empowers them and how they envision #DigitalHifazat – situated within their specific sociopolitical identities and experiences.[39]

**'Web Wonder Women'**

The Union Ministry of Women and Child Development on January 9, 2018 launched an online campaign, 'Web - Wonder Women' also known as '#www'.[40] The online campaign, 'Web Wonder Women' was organized by the WCD Ministry with an aim to celebrate the exceptional achievements of these women who were selected after an extensive research process. Organized in collaboration with Twitter India and Breakthrough India, the event aimed to recognize the fortitude of Indian women stalwarts from across the globe that has used the power of social media to run positive and niche campaigns to steer a change in the society.[41]

[39] Feminism in India, DigitalHifazat – Campaign To Combat Cyber Violence Against Women In India, November 16, 2016, https://feminisminindia.com/2016/11/16/digitalhifazat-campaign-cyber-violence-women-india/

[40] RUPALI PRUTHI, Women and Child Development Ministry launches '#www: WebWonderWomen' Campaign,JAN 10, 2019,https://www.jagranjosh.com/current-affairs/women-and-child-development-ministry-launchesweb-wonder-women-campaign-1547117898-1

[41] India Today Web Desk,Web Wonder Women campaign: Centre honours 30 women stalwarts for driving social reforms,March 7, 2019, https://www.indiatoday.in/education-today/gk-current-affairs/story/web-wonder-womencampaign-union-ministry-womens-day-1472201-2019-03-07

## PART VI- CONCLUSIONS

The main aim of cyber socializing is to give the users opportunity to socialize without actually going in person to the social gatherings.The introverts who are afraid to socialise in a social gathering, cyberspace provides a medium for them to socialise online. But this is not a hazard free zone. The main drawback of cyber socializing is the uncertain reliability of the "virtual friend". Majority of the people must have faced some type of cybercrime in their life.The two main reasons which attribute towards the growth of online victimization of women are: absence of proper gender sensitive universal cyber laws and lack of awareness of the safety modes among users.[42] India has a long way to go before it can claim to have a robust legal framework to address violence women face online. It has made some forays in this regard, but the fragmented nature of the provisions and retrograde social attitudes to the problem takes away any real impact the law can have. The Ministry of WCD is looking to tighten the law, and bridge the gap between the existing provisions of the IPC and ITA in addressing sexual violence online against women.[43][44]Unfortunately, there are less laws and policy guidelines to regulate cyber space and this insufficiency gives full freedom to the perpetrators. This is a perfect example of how ignorance of cyber-social rules and norms coupled with weak laws can encourage criminalization in the online socialization.[45] It is the job of the legal system and regulatory agencies to keep pace with the Technological developments and ensure that newer technologies do not become tools of exploitation and harassment. Governments can take legislative measures that ensure human rights; especially women's rights are protected online just as they are physical spaces. Legislation should not just protect users; however, it should also educate and inform all groups on how to exercise their communication rights. Cybercrimes against women are still taken lightly in India, mostly because in general the respect towards women in our modern society is on a decrease also a lot of people are unable to come to terms with the fact that even posting images of someone online in a crime. Cyber crimes such as morphing, e-mail spoofing do-not have a moral backing in society and hence are taken lightly. For dealing with such cases we need a cyber army who knows are well versed with the latest technology and advances, can deal these cases more efficiently and within a short span of time so that justice can be served. While making strategies to curb cyber crime, women who have faced cybercrime must be given a chance in discussion as they understand the gravity of the crime privately. Women who have faced these crimes goes through a severe trauma and are not able to open up infant of the male authorities,

---

[42] Halder, Debarati & Karuppannan, Jaishankar. (2009). Cyber socializing and victimization of women,https://www.researchgate.net/publication/47748969_Cyber_socializing_and_victimization_of_women

[43] Submission on Online Violence Against Women to the Special Rapporteur on Violence Against Women, November

[44] ,https://itforchange.net/submission-on-online-violence-against-women-to-special-rapporteur-on-violence-against-women

[45] Supra2

having a female judge or prosecutor might help them get comfortable to share their story. The gap between the legal remedies provided in the Acts i.e. (IPC AND ITA) need to be filled, so that a strong legal framework will be formed to address violence faced by women online.

Therefore, to eradicate cyber crime completely not only stringent penal provisions are needed but also a change in the mind set of people is must. A proper education system which will openly discuss about the problems faced by women without making it a taboo is very important. Such changes cannot come from a single block of society but people, Government and NGOs etc.. need to work together to bring forth such changes.