LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +919310053923 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

GENDER ATTENTIVE LIABILITIES OF THE DIGITAL WORLD AND IT'S POTENTIAL SOLUTIONS IN INDIA AND ABROAD*

The Cyberspace has come a long way since it's inception as ARPANET (Advanced Research Projects Agency Network), originally funded by the U.S. Department of Defense the 1960's. It has now become an unprecedented all inclusive platform which connects people from every corner of the world. From banking services to entertainment websites to educational articles to social media such as Facebook and Instagram, the cyberspace has crafted a multi-dimensional virtual world which has vociferously entangled itself into every iota of our public and private lives. The problem today is that the platform of cyber space has now also become open ground for often unchecked racism, sexism, communalism etc. The ensuring of safety to woman has always been a national and global priority, today more than ever.

Understanding the technicality of the problem

The UN Committee on the Elimination of Discrimination against Women (CEDAW) General Recommendation 19 defines gender-based violence as "violence that is directed against a woman because she is a woman or that affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty"[1] . The CEDAW General Recommendation 35 extends the definition coined under General Recommendation 19 by adding that "...Gender-based violence against women ... manifests in a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology mediated settings". And "Gender-based violence against women

* **Arinjoy Chaudhury & Vidur Mehta, Student, Symbiosis Law School, Pune.**

[1] CEDAW (1992), "General Recommendation No. 19" (11th session, 1992), available at http://www.un.org/womenwatch/daw/cedaw/recommendations/index.html

occurs in all spaces and spheres of human interaction, whether public or private ... and their redefinition through technology-mediated environments, such as contemporary forms of violence occurring in the Internet and digital spaces"[2] .

The UN General Assembly (UNGA) 2013 Consensus Resolution on protecting women human rights defenders contains language on technology-related human rights violations: "information technology-related violations, abuses and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights"[3].

After a detailed skim through of the ways in which multilateral, Asian and EU institutions define cyber violence and hate speech online against women, it may be advantageous to explore how the phenomenon is theorized in academic circles and in civil society. A large number of definitions, either legal or coined by activists or academics, and salvaged by media, compete and contribute to the fact that the phenomenon of cyber violence and hate speech online against women is problematic to grasp and understand. Moreover, other actors such as Internet intermediaries and other institutions also produce a lexis that influences users and policy makers.

Cyber crime studies have categorized cyber crime into:

1) Traditional criminal activities that are expanded or heightened by the Internet;

2) Traditional criminal activities that are generalized and 'radicalized' by the Internet and;

3) Criminal activities that are created by the Internet[4]. In the chapter on Impact, we will see that this applies to cyber violence against women as well.

[2] CEDAW (2017), "General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19", available at https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf Policy Department for Citizens' Rights and Constitutional Affairs

[3] UNGA (2014), "Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: Protecting women rights defenders". (A/RES/68/181). Available online: http://www.gender.cawater-info.net/publications/pdf/n1345031.pdf

[4] Gillespie, A (2015), "Sexual exploitation", in T Buck (ed.), International child law. 3rd edn, Routledge, London, pp. 333-383

It is an open truth that many academics emphasize the need for reframing the terminology used by media to describe the different forms of cyber violence and hate speech online against women forms of victimization.

The term 'Revenge pornography' especially is being discussed as describing the perpetrator's experience rather than the Victim's abuse. Therefore, the terminology describing this novel form of victimization is still evolving.

The International Center for Research on Women (ICRW) is leading a Technology-facilitated gender based violence Project in partnership with the World Bank and has developed an abstract framework that helps us to visualize the scope of cyber violence and hate speech at a glance.

• 'Hate speech' "lies in a complex nexus with freedom of expression, group rights, as well as concepts of dignity, liberty, and equality (...) hate speech (is defined) as any offense motivated, in whole or in a part, by the offender's bias against an aspect of a group of people[5]".

• Online sexual harassment, refers to a great variety of harassing behaviors, "including cyberbullying,

cyberstalking, gender-based hate speech, image-based sexual exploitation and even rape threats".

• The term cyber stalking is generally defined as an extension of offline forms of stalking using electronic means. But the term is being discussed by experts as to be only applicable to a legal definition requiring "repeated behaviours that cause fear". Some scholars would rather use terms such as ''less severe methods of online pursuit'' or ''cyber-obsessional pursuit'' that may or may not spiral into cyberstalking.

• 'Revenge pornography' is a form of technologically aided sexual violence, wherein a perpetrator disseminates nude and sexually explicit photos or videos of an individual without their consent. Henry and Powell (2018) conceptualize the perpetration as "image-based sexual exploitation" whereas McGlynn, Rackly and Houghton (2017) name it "image-based sexual abuse"[6]. Professors Nicola Henry and Anastasia Powell argue that the phenomenon should be thought of as "image-based sexual exploitation" because it "(a) captures the broad range of perpetrator motivations, rather than simply assuming that all revenge porn is uploaded for "revenge" purposes; (b) encompasses images that may not be considered pornographic, but are used for pornographic

[5] Silva, L. and al. (2016), "Analyzing the Targets of Hate in Online Social Media", available at https://arxiv.org/pdf/1603.07709.pdf

[6] McGlynn C., and Rackley, E., and Houghton, R.A. (2017), "Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse", Available at https://ssrn.com/abstract=2929257

reasons; and (c) includes a broader range of contexts in which the imageries were originally produced (e.g., "selfies")"[7].

Internet intermediaries also come forward with their own definitions. These are mainly for internal use in defining company policies towards cyber violence and hate speech. In the below two examples:

• The social media platform Facebook defines 'hate speech' as "anything that directly attacks people based on what are known as their "protected characteristics" — race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disability or disease"[8].

• In its section for rules and policies, the social media company Twitter defines "abusive behavior "as an attempt to harass, intimidate, or silence someone else's voice", it further defines "non-consensual nudity sharing" as "sharing explicit sexual images or videos of someone online without their consent"[9].

Violations of privacy, the subsequent glossary is an easier way to understanding the ambit of cyber crimes against women-

• Revenge porn or image-based sexual abuse/exploitation is the type of behaviour consisting of accessing, using, disseminating private graphical or video content without consent or knowledge, content sent by means of 'sexting' can also be shared without consent.

• Creepshots, upskirting or digital voyeurism consists of perpetrators taking non-consensual photos or videos of women's private body parts and sharing them online.

• Doxing refers to researching/manipulating and publishing private information and details about an individual, without their consent as to expose, shame and often access and target the person in "real life" for harassment or other types of abuse.

• Impersonation is the method of stealing someone's identity so as to threaten or intimidate, as well as to dishonor or damage a user's reputation.

[7] Henry N., Powell, A. (2018), "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research, Trauma, Violence, & Abuse", vol. 19, 2: pp. 195-208. First Published June 16, 2016.

[8] Facebook News Room (2017), "Hard Questions: Who Should Decide What Is Hate Speech in an Online Global Community?", https://newsroom.fb.com/news/2017/06/hard-questions-hate-speech/

[9] Twitter Help Center (2017), "About intimate media on Twitter", available at https://help.twitter.com/en/rules-and-policies/intimatemedia

• Hacking or Cracking refers to the act of intercepting private communications and data, it can affect women especially in the form of webcam hacking.

• Cyber stalking is the act of spying, fixating or even compiling information about somebody online so as to communicate with them against their will. The tactic is often used and analyzed as an extension to intimate partner violence.

Harassment

• Cyber bullying consists of recurring behaviour using textual or graphical content with the aim of frightening and depressing someone's self-esteem or reputation.

• Threats of violence, including rape threats, death threats, etc. directed at a victim or their offspring and relatives, or incitement towards physical violence.

• Unsolicited receiving of sexually explicit materials.

• Mobbing, refers to the act of selecting and targeting someone to bully or harass through a hostile mob deployment, sometimes including hundreds or thousands of people.

Sexist hate speech

• Sexist hate speech is defined as expressions which spread, provoke, promote or validate hatred based on a person's sex.

• uploading and sharing violent content consist of portraying women as sexual objects or targets of violence can be very detrimental also.

• Use of sexist and insulting comments, abusing women for expressing their own views and for turning away sexual advances.

• Pushing women to commit suicide.

Direct violence

Some forms of cyber violence against women have a straight impact on their immediate physical safety:

• Trafficking of women using technological means such as recruitment, enticing women into prostitution and sharing stolen graphical content to advertise for prostitution.

• Sexualized extortion, also called sextortion and identity theft resulting in physical abuse.

• Online grooming consists of setting up an online abusive relationship with a child, in order to bring the child into sexual abuse or child-trafficking situations. The term "grooming" is criticized by victims, as it covers the child sexual abuse dimension of the act.

• In Real-World Attacks is defined as cyber violence having repercussions in "real life".

Legislation and regulations adopted around the globe

Measures to control violence against women is the need of the hour for each and every nation state and it is a pressing issue which must be resolved immediately with the right kind of acts and statutes being drafted by the nations government. The dilemma here is that the era of cyber crimes is a relatively new one especially for the developing countries and understanding the complexities behind each crime is a tedious task. Hence there has not been a really sound and fitting bill as yet to curb these atrocities, but there have been major efforts from each and every government to try and make a difference. We can critically analyze the different kind of legislations, regulations and recommendations being made across the world in this regard.

Europe

Various nations in the European continent have recently adopted legislation targeting forms of cyber violence against women; for instance provisions criminalising revenge porn have been enacted in the U.K., France, Germany and Malta, with policies currently pending in Ireland and Slovenia. While this is a step in the right direction, studies suggest that current legal and policy approaches in the EU fail to adequately capture the social and psychological harm resulting from the use of sexual imagery to harass, coerce or blackmail women.[10]

Moreover, research shows that the response of the criminal justice sector to women victims is not adequate, like in the U.K., a total of 1160 incidents of revenge porn had been reported over a period of six months but out of these about 60% led to no further action against the criminal.

In 2013 the End Violence against Women Coalition (EVAW) gathered accounts on enforcement and prosecution of 'violence and harassment' online, stating concerns that criminal justice authorities took a contrary, and less effective, approach to violence and harassment orchestrated online compared to offline. Several participants themselves had experienced 'wholly inadequate police responses' when reporting a crime perpetrated online.[11]

10 Henry, N. and Powell, A. (2015). Beyond the 'sex': Technology-facilitated sexual violence and harassment against adult women. Australian and New Zealand Journal of Criminology, 48(1), 105.

11EVAW (2013). New Technology: Same Old Problems. Report of a roundtable on social media and violence against women and girls.Pg.5

Studies evidence these issues, revealing women's frustration with the police who tend to treat each individual online communication as a discrete act, instead of actually understanding the consequences caused by each act on the victim. Furthermore, society ends up blaming the victims, especially in cases of revenge porn, demonstrating a lack of understanding and awareness. This is proved by the fact that more than half of stalking and cyber stalking victims did not acknowledge their own experience as a crime.[12] This inadequate criminal justice response can be attributed in part to the false dichotomy between online and offline Violence against women, which results in police minimising the harms of cyber Violence, and constructing victims' experiences as "incidents" rather than patterns of behaviour over time.

However, it is not completely bleak and there a few victories here and there showing a ray of hope for better legislation and investigation in regard to cyber crime as a whole. In the U.K., in April 2015 it became a criminal offence with maximum two-years imprisonment to share private sexual photographs or videos without the subject's consent providing the intent of causing distress to those targeted.[13] In September 2016 it was announced that more than 200 people had been prosecuted since the law came into effect which definitely showed some substance in the form of policy implementation.

Subsequently in 2016, France adopted the 'Digital Republic Law,' which entails a harsher sanctioning of those found guilty of revenge porn. Under new legislation criminals are faced with a two year prison sentence or an exorbitant fine. Similar provisions were also brought into force in Germany, which in 2014 made it an offence to keep intimate pictures of a partner after they have asked for their deletion.

Besides these legislation there have been a few research and interventions being conducted as well so that the public at large can be convinced about the magnitude of these offences and understand that it is not okay to suffer atrocities like these.

In 2009, Britain. Launched The National Centre for Cyberstalking Research, which aimed to provide research and analysis into the prevalence, motivations, impacts and risk assessment of cyber violence against women. In 2011 the centre published the results of a study on the

12 Nobles, M.R., Reyns, B.W., Fox, K.A. and Fisher, B.S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. Justice Quarterly, 31(6), 53-65

13 Crown Prosecution Service guidelines on prosecuting the offence of disclosing private sexual photographs and films

prevalence, nature and impact of cyber stalking and has conducted a survey investigating the impact and prevalence of revenge porn.[14]

Even developing nations like Slovenia have joined the fight by launching projects like 'CYBERVAW', which aim to develop awareness-raising and education activities that spread a clear message of zero tolerance, with a specific focus on prevention of gender-based cyber violence.[15]

In totality there is a lack of research and empirical data to analyze the entire continent as a whole because there is great disparity between nations. Legislation must be made in relation to the Istanbul Convention and the International Human Rights legal framework so that all the EU nations can start their fight against cyber violence against women because there is still a long way to go.

Americas

Studies have shown that the USA has the highest amount of cyber specific legislations in the world which may not be the most surprising fact considering the development, but the important question is that has it been implemented everywhere and is it useful as the country is geographically very big. The U.S communications and decency act, 1996 act differentiates child pornography and have both federal and state laws on the subject. Besides that computer fraud and abuse act deals with hacking as an offence. The most important statute in this relation is the section 223(a) title 47, USC which does not allow any pictures of telephonic communications with regard to any former partner to be made.

This was legislation, but implementation is a whole other story. In 2014, the journalist Amanda Hess accounted her attempts to pursue the American criminal justice to end two cases of cyberstalking. The first time she went to police, in 2009, it was after a reader began issuing graphic rape threats online which then converted to phone calls. The police refused to take action unless the man showed up at her apartment. Eventually, she was able to use a then-recent change to the law that allowed her to file for a civil protection order in a family court. The order lasted for a year, after which she was contacted and harassed once again.

14 Maple, C., Short, E., Brown, A. (2011). Cyber stalking in the United Kingdom: An Analysis of the ECHO Pilot Survey

15 Report of the Office of the High Commissioner for Human Rights on ways to bridge the gender digital divide from a human rights perspective

Research into online abuse by Pew in 2014 said that 40% of people had experienced some form of harassment on the internet – and that young women were among the most commonly targeted groups.[16]

In June 2015, the US Supreme Court in a landmark judgment of Elonis v. United States[17], decided in favour of Anthony Elonis, who posted graphic warnings on Facebook of his desire to kill his estranged wife, saying they weren't a crime if he didn't intend to follow through and the trial hadn't established Elonis' intent. This was a decision that had been overturned by the Supreme Court as the Pennsylvania court held Elonis liable. That is discomforting to victims of online harassment, who still face uninformed law enforcement officers when they report, a patchwork of laws that makes harassment difficult to prosecute across state let alone international lines, and a civil process that is expensive and time-consuming even when it works at all.[18] Professor Danielle Citron suggested a few solutions which include ensuring that laws are technology agnostic; allowing prosecutors to present to judges and juries a totality of the abuse; and increasing penalties for those convicted.

When we look at Latin America, a good nation to consider as a case study would be Columbia. Just like any other nation Columbian Internet users face all the stigma and abuse, like stalking, revenge pornography and blackmail. It is just that the abuse is escalated because more often than not it is caused by Paramilitary groups that bring cyber abuse to the victims home. Olga Paz Martinez, coordinator of the Take Back the Tech' project in Colombia, says such online violence is often directed against women's rights campaigners and in particular those who speak out about sexual violence against women.[19]

In 2009, Colombian feminist organisation Mujeres Insumisas was victim to a number of online threats about their social work and campaigning for women's rights. The abuse occurred for a period of 3 years through emails and mobile phone messages. Besides that, at least three women working for the NGO were victims of sexual violence, harassment and stalking during this period.

[16] The Guardian : Online Abuse, how different countries deal with it, (4.1.19), https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it

[17] Elonis v. United States, 575 U.S. 875 (2015)

[18] New York Times, Supreme Court Overturns Conviction in Online Threats Case, (2.1.19), https://www.nytimes.com/2015/06/02/us/supreme-court-rules-in-anthony-elonis-online-threats-case.html

[19] Gender Equality Observatory for Latin America and the Caribbean ECLAC: http://www.cepal. org/oig/

Over the course of 3 years paramilitary groups sent a total of 12 emails telling the agency to stop their work. The reasoning for the same is the deep cultural root of the country which puts the man on a pedestal and does not really have a place for the woman. It is very popular in Columbia that a woman returns to her former partner because of revenge pornography or blackmail. It is also considered normal for the woman to be stalked or harassed and if she speaks up those close to her are told to keep her quiet. In 2008, a landmark piece of legislation was introduced in Colombia which addressed violence against women, but there is no specific mention of technology-related violence and the law is ill-equipped to help people who are the victims of online harassment and abuse.[20] Reform must take place as Columbia is one of many countries in Latin America where this is prevalent and the entire region must break the shackles of barbaric culture and move to a system of gender justice.

Asia

Asia consists of more than one-third of the world population and hence even though, consists of developing countries mostly, the continent has the highest number of cyber user as well. We will not include India in this segment because we have conducted a seperate study for India and its judicial pronouncements in this regard.

In South Asian countries the amalgamation of Buddhist, Confucian, Hindu, Islamic and Christian traditions have shaped the personalities of women and determined their social status. Rigid cultures and patriarchal attitudes which devalue the role of women, result in the wide spread occurrence of violence against women. The family structure, in which the man is the undisputed ruler of the household, and activities within the family are seen as private, allows violence to occur at home. Earlier they would be traditional forms of violence like honour killings and domestic violence but now with newer technology, there are newer methods of hatred being spread, such is the nature of man. This is where cyber violence comes into the picture where in women are specimens to atrocities like cyber bullying and stalking.

We must focus on China, a country that has more internet users than any other country with 688 million and counting. China is the most fertile ground for online abuse to women, with cyber

[20] Online Abuse, how different countries deal with it, The Guardian, (3.1.19), https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it

bullying and cyber stalking on an imminent rise all the time. The most notorious form is the so-called “human flesh search engine”, by which internet users club together to identify and then publicly humiliate online targets who have been accused of anything from corruption to infidelity or animal cruelty. It does not matter if the allegations are true or not, these so called keyboard warriors will bully as a hobby. This is not a gender based crime but takes place in China so frequently that a lot of women end up suffering as a result.

Chen Yaya, a research assistant with Shanghai Academy of Social Sciences, stated that there has been an alarming increase in the number of women and girls becoming victims of such violence, which not only violates women and girls' rights, but also affects their safety in cyberspace. For example, female netizens, especially those who have suffered from online violence, are not willing to "speak openly" on the Internet.[21]

In recent years, China, in collaboration with UN agencies and international organizations, has launched many programs and activities with the purpose of raising the public's awareness of, and the need to, eradicate cyber violence. One such project was launched in 2013 by Shanghai Academy of Social Sciences, and that project urged government departments to take effective measures to eliminate gender-based discrimination occurring on new-media platforms.[22] The project's staff issued a proposal that emphasized the importance of promoting gender equality and improving self-discipline when giving opinions on various websites.

When we look at Indonesia, a country with a significantly large population on the brink of development, it is the perfect match for cyber violence. Komnas Perempuan recorded a total of 65 cases of cyber violence against women last year and categorized the various types of incidents: recruitment, online defamation, malicious distribution, infringement of privacy, illegal content, hacking, cyber-harassment and cyber-grooming.[23] In 2017, Indonesia saw the launch of certain websites like ‘ayopoligame.com’ which was a form of online prostitution with a religious tenet. It was a form of online polygamy with a pinch of domestic violence. There has been a rise in young girls being abused online and as recent as 2017, a paedophile group had been uncovered which had a network of young girls online.

[21] Women of China November 2017 Issue, (2.1.19), http://www.womenofchina.cn/womenofchina/html1/exclusives/1802/2178-1.htm

[22] https://www.cipe.org/blog/2018/04/12/what-can-be-done-to-effectively-combat-cyber-violence-against-women-and-girls/

[23] Report of National Commission on Violence Against Women, 7th March, 2017

Even though the country has an effective national commission known as Komnas Perempuan and cyber violence is mentioned in the electronic information and transaction law, it is not being able to cope with the number of victims to cyber offences and there is strict need for reform by the Judiciary and Legislature.

Pakistan is no stranger to cyber violence against women as the country has had a history of inadequate care being given to women in regard to basic offences as stated by the Human Rights report of 2015. There had been some reform by the Pakistani government after this report but soon the perpetrators found a way to abuse women, sitting behind a screen and the battle for empowerment is still going on. Thankfully, the Prevention of Electronic Crimes Bill (PECB) 2015, adopted by the National Assembly of Pakistan, contains a special provision for the protection of women online. The article makes it punishable by law to threaten a woman with sexual violence or post sexually explicit images of a woman online without her "express or implied consent." If cyber activity "threatens injury to reputation, her existing state of privacy, or puts her in fear for her safety," the offender could face imprisonment for up to a year, a fine of one million rupees or both. [24]

The current situation in India

Our great nation has been battling archaic, patriarchal and regressive mindsets for decades now. The digital footprint of these socially backward thought processes surface on the internet as the different forms of cyber crimes against women we have discussed earlier. The following are some statistics which global security firm Norton disclosed after a semantic survey in India in the year 2017 under which thousands of people had participated-

Data from the survey showed that people below the age of 40 are experiencing the remarkably high levels of abuse, with 65% reporting incidents of the online abuse and harassment. Disturbingly, 87% of people with mental health issues and 77% with body shape or weight issues had experienced some kind of abuse or harassment. The impact on the real world from digital abuse was also looked at in the study and found that 28% had experienced difficulties at work or studies, 27% experienced an impact on relationships with friends, 26% experienced depression or

[24] Prevention of Electronic Crimes Bill (PECB) 2015 https://thediplomat.com/2016/04/the-cyber-harassment-of-pakistans-women/

emotional stress and 24% reported losing friends resulting from being targeted online. The findings have encouraged calls for more action from service providers and social media platforms to be clearer in defining acceptable conduct and to be stronger in their response to users who choose to breach conduct guidelines.[25]

Another very sad aspect of this predicament is that an exponentially large number of minors are falling victim to online harassment. Teenagers and kids make up most of the internet's daily visitors and in a report compiled by comparitech.com it was found that Indian children are the most cyber bullied in the world. The Comparitech report, which analyzed an Ipsos international survey of adults in 28 countries, said that the number of parents complaining about their children being cyberbullied is increasing[26]. The survey had conducted around 20,793 interviews between March 23 and April 6, 2018, among adults between ages of 18-64 in the US and Canada, and adults between age 16-64 in all other countries.

Landmark Cases

Some noteworthy cases to remind us of the grim reality of the situation-

I) Manish Kathuria Case[27]

The first reported case of cyber-stalking in India which brought about the 2008 amendment to the IT Act,the Manish Kathuria case involved the stalking of a woman named Ritu Kohli. Kathuria stalked Kohli on a chat website, abused her by using obscene language and then circulated her telephone number to various people. Later, he began using Kohli‟s identity to chat on the website "www.mirc.com". As a result she started receiving more than forty obscene telephone calls at any hours of the night over three consecutive days. This situation convinced her to report the matter to the Delhi Police. As soon as the complaint was made, Delhi Police traced the IP addresses and arrested perpetrator under Section 509 of the Indian Penal Code. The IT Act was not besought in the case, since it had not come into force at the time when the complaint was filed. While there is no record of any subsequent proceeding, this case made Indian legislators wake up to the need for a legislation to address issues like cyber-stalking. Even then, it was only in 2008 that the Section

[25] The Cyber Smile Foundation, NORTON BY SYMANTEC SURVEY IN INDIA REVEALS 8 OUT OF 10 INTERNET USERS EXPERIENCE ONLINE ABUSE, (8.1.19) https://www.cybersmile.org/news/norton-by-symantec-survey-in-india-reveals-8-out-of-10-internet-users-experience-online-abuse

[26] The Wire, Indian Children Most Cyber-Bullied in the World: Study, (7.1.19), https://thewire.in/tech/indian-children-most-cyber-bullied-in-the-world-study

[27] Manish Kathuria And Others vs State Of Punjab And Others (2014)

66-A was introduced. As a result, now cases are being reported under this section as opposed to Section 509 of the Indian Penal Code, as was the case where a Delhi University student was arrested for stalking a woman hailing from Goa by creating fake profiles on social networking websites, uploading pictures on them and declared her to be married to him. It is hoped that the decision in this would favour the victim.

ii) Karan Girotra V. State[28]

The only reported case which went in a full fledged manner to the judiciary on cyber-stalking is also merely an application to grant anticipatory bail. this case dealt with a woman called Shivani Saxena, whose marriage could not be consummated; as a result she filed for divorce by mutual consent. In the meanwhile, she came across Karan Girotra while chatting on the internet, who told her he loved her and wanted to marry her. On the pretext of introducing her to his family, Girotra invited Saxena over to his house, drugged her and then assaulted her sexually. He kept assuring her that he would marry her and began sending her obscene pictures from the night she was assaulted. He also threatened to circulate the pictures if she did not marry him. As a result, an engagement ceremony took place between the two after which he continued to assault her and eventually called off the engagement to her. As a result, Saxena filed a complaint under Section 66-A of the IT Act.

Though the Court rejected the plea of anticipatory bail on the ground that nude and obscene pictures of Saxena were circulated by Girotra, an act which requires serious custodial interrogation, nonetheless it made some scornful remarks. According to the Court Saxena had not disclosed her previous marriage to Girotra merely because she agreed to perform the engagement ceremony, even though such mention was made when Girotra had first declared his love to Saxena. The Court also took noted that there was a delay in lodging the FIR by Saxena. What is more shocking is that the Court held that Saxena had consented to the sexual intercourse and had decided to file the complaint only when Girotra refused to marry her.

This case brings to light the attitude of the Indian judiciary towards cases involving cyber-stalking. It is appalling that factors as redundant as a simple delay in filing the FIR have a huge bearing on

[28] Karan girotra vs state and others (2012)

the conclusion of the case. It is for this reason that more stringent legislations are the need of the hour.

Conclusion

The first step to adequately ensure preliminary safety against cyber crimes is knowing the IT related laws of the country. The Indian Penal Code has a host of articles that deal with the issue of cyber crimes. The Main Ones being-

Section 354A of the IPC:
Posting lewd comments on social media makes one liable under this law and can be punished with one-year imprisonment and fine. In addition, posting/messaging content connected 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.
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 non consensually captures an image/video of a woman engaged in a private act. Such an act is punishable by one to three years of imprisonment along with a fine. This provision can be invoked especially in cases when the woman does not expect to be observed by the accused.
Section 354D of the IPC:
This provision of the IPC deals with what we refer to as "online stalking". The provision covers the grounds of a case where an effort to contact a woman is made through the internet, e-mail or any other form of electronic communication with the intention of establishing personal natured interaction despite her visible disinterest. Such an act is punishable with three years of

imprisonment on the first count being followed by five years of imprisonment on the second count both of which are in addition to a monetary fine.

Section 499 of the IPC:

Any individual who is certain that his/her reputation is being harmed by a visible representation published on the internet can invoke this provision which accounts only for remarks on social media or obscene images or videos posted for public consumption. Under this provision, defaming a woman online will send the perpetrator to jail for a period of two years.

Section 503 of the IPC:

In the circumstance of an individual threatening a woman with the intention to either alarm her or harm her reputation, the former is liable to be penalized with a jail sentence of two years.

Section 507 of the IPC:

Under this provision, an individual who acts so as to intimidate or threaten a woman by anonymous communication is liable to be punished with two years in prison.

Section 509 of the IPC:

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

Section 66E of the IT Act:

Publishing a visual image of a person in print or electronic form that would result in the violation of the privacy of the individual which can lead to three years imprisonment or a fine ranging from Rs 2 lakh to Rs 10 lakh. According to this provision of the IT Act, while the first conviction would result in three years of imprisonment, a second conviction under the same provision can lead to a jail term spanning seven years along with a similar fine.

Thus schools and colleges must strive towards raising awareness about these issues either by introducing it in it's curriculum or simply as drives and workshops. The subjects of computer science and computer applications in schools can have specific chapters regarding safety on the internet and it's laws. Colleges can hold seminars for teaching the students how to navigate the internet without falling prey to cyber bullies or online harassers.