Cybercrimes With Gender Lens – Laws & Remedies©

By Red Dot Foundation & Cyber Saathi Foundation

Executive Summary:

Women and children are soft targets for crimes, more so with cybercrimes. The National Crime Records Bureau ("**NCRB**") reports along with other studies unequivocally point to the increasing virtual gendered violence that impacts women and children physically, psychologically and financially. In particular it impedes the exercise of their fundamental rights of speech and expression and also infringes on their right to privacy.

Cyberstalking, cyber harassment, cyberbullying, using the online domain as a weapon to extort / blackmail victims, in particular with sextortion or what is referred to as 'revenge porn' are some recurring cybercrimes that particularly impact women and children. Such online gender-based violence has short and long-term impact on young people's mental health and wellbeing. The corona virus ('COVID') pandemic increased reliance on the digital medium and a natural consequence of such increased usage was a huge spurt in cybercrimes. Women and children were again a large target audience for the cybercriminals. The findings offer an indication that online sexual harassment is specific to the individual and depends on a variety of intersecting factors, including actual or perceived gender, gender identity, sexual orientation, race, religion, special educational needs, or disability. Whilst so, awareness of cybercrimes and remedies to combat them and also the means to avail of such remedies is abysmally low. This leads to further victimzation, as reports of cybercrimes are rarely filed. The available statistics therefore is barely a reflection of reality.

With the increase in the number of cybercrimes, predominantly against young adults and women, Cyber Saathi an initiative of N.S. Nappinai, in collaboration with Red Dot Foundation formulated and developed a unique awareness program titled **"Cybercrime Awareness through Gender Lens"**, (with N. S. Nappinai providing the domain expertise on Cyber laws and Ms. Elsa Marie D'Silva providing inputs on gender sensitization).

The program focused on providing knowledge & awareness about cybercrimes and remedies available in law, whilst also focusing on prevalent gender norms and stereotypes and how this influences interactions on the online space. This paper also addresses predominant types of cybercrimes emerging in India, before and after the Covid-19 pandemic, the state of cybercrime awareness in India, the level of awareness of gender inequality and gender sensitivity in India, which impacts online conduct.

It also discusses the current developments and interventions tackling gender inequality and injustice and fostering safer online environments, as well as the role of law and agencies and how they can reduce the increasing rates of cybercrimes and the issue of gender inequality.

The paper also addresses some of the positive outcome of the **"Cybercrime Awareness through Gender Lens"** awareness program including the participants increased knowledge on digital rights and gender equality after having attended and participated in the awareness session as well as a clear and better understanding and access to information on various gender issues and cybercrime and remedies available, are some of the positive outcomes and feeds back.

****

Introduction

Digital technology has pervaded daily life. In the 21st century, cybercrime has grown to be one of the main safety issues affecting governments, businesses and individuals.

Cybercrime refers to any illegal activity committed by the use of electronic communications networks, such as the Internet, against individuals or groups with a criminal intention to purposefully damage the victim's reputation or to impose physical or mental harm on the victim, either explicitly or implicitly. Cybercrime has not been defined in any legislation in India. 'Cybercrimes' could, in general be described, "as a category of offences committed using computers or computing devices as a source or weapon" (Nappinai N. S., 2017).

Online sexual harassment involves a wide range of practices that utilise digital material (e.g., images, videos, posts, comments, pages) on several different platforms (private or public). It can cause an individual to feel threatened, abused, intimidated, humiliated, hurt, sexualised or discriminated against. Some of the major crimes to describe and discuss online gender-based harassment include, defamation, email spoofing, phishing, morphing, trolling, sextortion, revenge porn and doxing (Blackwell et al., 2017; Citron & Franks, 2014; Hardaker, 2010; Mirchandani, 2020). Body shaming; name calling; vilification of reputation; propagating stereotypes; instigating violence against women; inducing victims to commit self – harm; issuing threats including of rapes and gang rapes or of murder are just some of the trends of online crimes impacting women (Cyber Saathi, 2020). There is a misapprehension that offences committed on digital medium do not have a physical ramification, which is patently incorrect. Crimes online have as much, if not higher impact than even physical crimes with the harms extending to physical, psychological and even financial (Nappinai N. S., 2021).

The European Union ("**EU**") Parliament's 2018 Study on 'Cyber violence and hate speech online against women' (2018) highlights the negative impact of online hate speech and crimes, against women and children, which causes physical long term harm to victims. Such cybercrimes have placed various health issues on women such as depression, hypertension, anxiety, and heart disease due to harassment (Patel, 2015). Cyberbullying has been linked to flaming, cyberstalking, denigration, masquerading, outing, trickery, and exclusion (Li, 2007). Although technology (such as social networking platforms, text messages, or emails), instigates these activities, online harassment victims also report disturbances to their offline lives, including emotional and physical discomfort, changes in the use of technology, and increased concerns about security and privacy (Duggan, 2017). Globally, studies show that around 41% of women who have experienced any form of online violence have feared for their personal safety in offline spaces as well. (Amnesty International, 2017).

Such harassment also usually occurs in a gendered context, with girls being more likely to be harassed than boys, and these incidents frequently lead to more detrimental outcomes for girls,

particularly for certain types of online sexual harassment. (Report of Child Relief & You ('CRY') on 'Online Safety & Internet Addiction', 2020).

Prevalence of Cyber crimes during the surge of Covid-19

There has been alarming new data available regarding the increase in viewership of Child Pornography in India given to the lockdown due to the global pandemic of the COVID-19 coronavirus.

A report of the ICPF shows a 95% increase in child porn consumption during March 2020. The Report indicates that there is an especially demand of Child pornography from North in New Delhi, Ludhiana, Raipura, Lucknow, Chandigarh, Agra and Shimla; in Central India in Raipur, Ranchi, and Indore; in the West in Mumbai, Thane, Pune and Ahmedabad; in the East in Imphal, Guwahati, Kolkata, Howrah and Shillong; in Southern India in Kochi, Bengaluru and Thiruvananthapuram.

Some of the Statistic provided by the India Child Protection Fund of April 2019:

- Males constitute 90% of CSAM users in India;
- Women constitute 1% of CSAM users in India;
- Browsers including Google Chrome, UC Browser, Firefox and Internet Explorer are some of the most used browsers to view CSAM;

The Childline Help line India received 92,000 calls from victims of sexual violence in 11 days (The Hindu, 2020). This data available indicates that the lockdown has endangered the safety of children and women too who are confined to their homes in which they are forced to remain in close proximity with their abusers.

The National Crime Records Bureau (2019) lists a total of 44,546 cases registered under Cyber Crimes in 2019, showing a significant 63.5% in registration of cybercrime cases over 2018 (being 27,248 cases).

As per The National Crime Records Bureau (2019), 60.4% of cyber-crime cases registered in 2019 had fraud as the motive. This was followed by sexual exploitation with 5.1% (2,266 cases) and for causing disrepute with 4.2% (1,874 cases).

Online violence targeted at women deters women from accessing and using the internet. This is especially alarming considering that there already exists a large disparity amongst women in India with respect to access to internet and mobile devices. According to the 2019 India Internet report, the female internet users are less than half as opposed to 258 million male users. Yet, women and girls are the larger targets for cybercrimes (CRY Report, 2020).

The National Crime Records Bureau (2019) lists 1645 cases women centric cybercrime cases in 2019, 1182 cases relating to offences of Publishing or Transmitting of Sexually Explicit Material, including such material depicting minors and 463 cases of other cyber offences against women such as Blackmailing / Defamation / Morphing / Fake Profiles etc.

By August 2020, 8,546 cybercrime cases were reported in Pune in just 8 months, exceeding the 7,700 cases reported in the year 2019. The Pune Police reported that the highest number of complaints (5,175) were under the subhead 'cheating frauds' including money transfer, online dating, and loan frauds. It is also postulated romance frauds had also increased during the pandemic. As a result of the lockdown due to the COVID-19 pandemic psychologists have also reported that many people, due to being secluded or feeling lonely have sought comfort in online relationships. This, although at first seemed easier for them to find romance online, yet it only made them more susceptible to online frauds (Madaan, 2020). It is also reported that a higher number of complaints involved instances of sextortion or sexual exploitation through blackmail (The New Indian Express, 2020). A slight increase of such cases was noted by the National Commission for Women (NCW), however, NGOs have also been inundated with incidents of online abuse, such as InfoSec Girls and Akancha Against Harassment. They reported seven to eight times more complaints than NCW and thus claimed that people are hesitant to formally file charges due to the associated social stigma and instead want these issues to be handled unofficially.

Online space creates several vulnerabilities for women. Patriarchy and the presence of other orthodox socio-cultural norms are also reflected within the online space, making women more prone to be victims of cyber-crimes. The NCRB data reveals that over the years, there has been a sharp increase in the number of incidences of cyber-crimes against women.

Some statistics released by the National Crime Record Bureau in 2019, with specific reference to cybercrimes crimes against women are as below (The National Crime Records Bureau (2019)):

Year	**Incidence of Cyber Crime (women centric)**	**Percentage Increase**
2019	1621	23.26
2018	1244	51.77
2017	600	NA

An increase in digital addiction due to the ongoing pandemic has also resulted in increased cases of cyberbullying among youth. Some statistics of cybercrime cases against minors as released by the National Crime Records Bureau 2019 areas below:

Sr NO.	**Offences against children in 2019**	**No. of Cases**
1.	Publishing or Transmitting of material depicting children in sexually explicit act	108
2.	Other Cyber Crimes against Children	62

Digital addiction can manifest, as excessive engagement with online games, social media, or porn. It can have different forms such as cyber-sexual addiction, cyber relationship addiction and information overload (Gupta, Swami & Nebhinani, 2020).

In India, there has been an exponential increase in cybercrime cases such as cyberbullying, cyberstalking and cyber extortion (more commonly known as revenge porn cases) cases (Nappinai.N. S. 2021 (cybersaathi.org)). However, the number of cases reported is not proportionate to the actual number of cases because often children do not report to their teachers and parents about getting bullied. According to Child Rights and You (CRY Report, 2020), 1 in 3 adults get bullied every day and most of them are aged between 13-18 years. According to the National Crime Records Bureau, there is a 36% increase in cyberstalking and cyberbullying cases in India.

The main reasons for individuals to engage in cyberbullying include ignorance of consequences and the nature of the action; other reasons could be anger, frustration, boredom, and a need for laughter (Shivashankar & Prakash, 2018). Often, bullies neglect the fact that it could have a long-lasting effect on the person being bullied. To fulfil their revenge, bullies go for cyberbullying. In most situations, a person who is bullied in an earlier situation becomes a bully to satisfy his or her thirst for revenge. There are also cases where an individual is unable to talk

directly to the victim and thus takes advantage of the anonymity of cyberbullying. Studies have shown that cyber bullying contributes to psychological symptoms such as aggression, depression, and low self-esteem (Hase et al., 2015; Schoffstall & Cohen, 2011) and its consequences have also been related to poor mental wellbeing, sex and drug use among adolescents (Oshima et al., 2012), which is troubling to researchers, educators, and clinicians. A study by Jain, Gupta, Satam, and Panda (2020) examined whether the susceptibility of cyberbullying has changed after the triggered Covid-19 pandemic lockdown among university students in the Mumbai region, India. It was found that the ages 17-18 were particularly vulnerable to cyberbullying and approximately 80% of this age group was cyberbullied during the lockdown period. Before the lockdown period, around 79% of the respondents that were bullied offline were also cyberbullied after the lockdown period, 66.67% of the respondents that were bullied offline continued to be cyberbullied even amidst the lockdown.

Given the trends that have emerged in the misuse of technology, Cyber stalking is another offence affects children and young adults. The persistent and unwanted attention by a man of a woman, which may become obsessive later on and results in the harassment and intimidation of that person amounts to stalking. If this same obsessive behaviour is committed either on or by using electronic technology, it could be classified, as cyber stalking. (Nappinai N. S., 2017)

Revenge porn cases / cyber extortion cases is another shameful trend of cybercrime that has permeated online and social media platforms. These are often shared on social media platforms and in some instances with explicit content pertaining to minors. Such offences also often include the recording of a physical crimes against persons by the perpetrator. The actions themselves are crimes and recording them is a crime in itself. Money victims of such revenge porn cases often report these offences as they are often blackmailed by the perpetrators into keeping silent and in some instance because of victim blaming / shaming. Cyber criminals in such cases believe that by body shaming and victim blaming, victims will be too afraid to report these offences and seek legal recourse.

Cyberbullying, cyber stalking body shaming and revenge porn are some offences that cyber culprits indulge in to silence their victims. It is a natural assumption that one would not what their privacy violated, least of all by a perpetrator, who has violated their privacy online. It important for victims of revenge porn or cyber extortion to know that even if the victim themselves have agreed to share bold or daring photos or videos this does not mean that others can be shared online. In order for victims of such offences to be able to seek their remedies in law it is also essential that we address issues such as the complexities in law and verbose provisions which may leave victims with a sense of uncertainty with respect to remedies available to them (Nappinai N.S. 2021).

Also, participants registered a general rise in the average time they spent on social media, from 3.72 h before lockdown to 4.01 h during the lockdown. Not only social media usage, but also

online gaming activity increased, and cyberbullying was 100% likely for individuals who played more than 10 games during the lockdown. Several studies have indicated the lack of awareness of cyber laws and cybercrimes among adolescents and young adults (Aparna & Chauhan & GJIMT, 2012; Mehta & Singh, 2013; Aggarwal 2015; Narahari & Shah, 2016). A finding by John (2020) indicated that the weakest aspect of higher education institutions in India revealed to be their lack of gender sensitivity. A study by Mokha (2017) also found that most of the respondents were not aware of crimes such as phishing, defamation, identity theft, and cyberstalking.

Why some gender targeted cybercrimes go unreported!

Most of the cybercrimes remain unreported due to the hesitancy and anxiety of the victims, particularly women and fear of defamation of their family's name. Many times, a woman considers herself accountable for the crime committed against her. As the identity of the perpetrator remains anonymous, women are more vulnerable to the danger of cybercrime and thus this allows the perpetrators to continuously threaten and blackmail the victim with various names and identities. Women fear that reporting the crime will make it harder for their family life; they also doubt whether they will gain the help of their family and friends and what society's impression will be of knowing about them. Due to these fears, women often fail to report such crimes, allowing the spirits of the culprits to get even stronger (Halder & Jaishankar, 2012).

It is also possible to attribute the recent rise in cybercrime against women to loneliness and spending more time on online activities which is further exacerbated by the impact of Covid-19. Thus, due to a change in lifestyles, women fall prey to social networking sites. On these websites or chatting apps, they make accounts and profiles and start making friends. They prefer to spend more time online without being conscious of the risks of cyberspace. This makes them more prone to targeted attacks online.

There is a lack of knowledge of 'cyber ethics' among individuals. Most people do not care about the policy guidelines (terms and conditions) for opening accounts or exchanging data on different websites or applications. Thus, without taking many precautions (such as setting proper security settings for social networking sites), they start exchanging personal information, sharing accounts, passwords, photographs, which makes them an easy target to cybercriminals.

Cyber Saathi,– "Cybercrime Awareness through Gender Lens" awareness programs for students in schools and colleges:

It is important for children and young adults to understand the threats and vulnerabilities that abound on digital domains – the space they occupy the most. With the current lockdown due to the COVID-19 pandemic, everyone has been moved to digital spaces. Students are spending more time online now than they did before the lockdown. From statistics available it is also clear

that students (i.e. children and young adults) are not only increasingly forming a larger portion of the demographic when it comes to victims of cyber crimes (CRY, 2020), as well as perpetrators.

The main focus behind the **"Cybercrime Awareness through Gender Lens"** sessions was to:

1. Reach out to this young demographic and equip them with a clear understanding of the possible cyber threats they may be susceptible to;

2. How to protect themselves from such threats and vulnerabilities;

3. What are the remedies available in law, in the event they fall prey to perpetrators online or if they know someone who has fallen victim to cybercrime offences;

4. Through the awareness and knowledge from the above session the participants could not only be a support system for themselves but also peer mentors for others, including family members, siblings and friends.

5. That through this process, the participants would then become "Cyber Saathis" or 'cyber friends' to others and also create a network of "Cyber Saathis" to increase awareness, reduce risks and create a support system amongst the younger demographic and so that they can reduced crimes against them;

Given the above scenario and the increasing number of cybercrime cases against young adults and women, Cyber Saathi an initiative of N.S. Nappinai, in collaboration with Red Dot Foundation formulated and developed a unique awareness program, **"Cybercrime Awareness through Gender Lens"**, (with N. S. Nappinai providing the domain expertise on Cyber laws and Ms. Elsa Marie D'Silva providing inputs on gender sensitization). This program aims at providing unique knowledge & awareness through online sessions for children, young adults, parents and teachers.

The **"Cybercrime Awareness through Gender Lens"** session focusses on prevalent gender norms and gender stereotypes and how this influences our interactions in the cyber domain, including gender targeted cybercrimes, how do people respond to such cybercrimes and also our treatment of victims of gender based cybercrimes.

The sessions also focused on creating awareness and knowledge of the various types of cybercrimes that affect children and young adults in the online space and help prepare peer mentors/first responders on the common cyber threats and susceptibilities faced online by young

people and adults, as well as provide victims with remedies to prevent young people and others from committing crimes due to ignorance.

Cyber Saathi empowers through knowledge and promotes responsible technology and respondent usage to ensure safe and protected digital spaces, with a specific emphasis on online safety for children and women. It intends to provide non-judgmental and non-preachy guidance with a strong emphasis on victim rights and empowerment through knowledge of remedies and the process of using them. This initiative is unique because it not only discusses protection from the viewpoint of the victim but also provides guidelines against the commission of crimes, highlighting what acts constitute criminal offences and punishments, thus deterring individuals from performing such criminal activities. Cyber Saathi also influences policymaking through research and publication of white papers intended to direct and raise awareness of cyber laws and legal aspects of emerging technologies to create a stronger Digital India.

Through the combined efforts of Cyber Saathi, an initiative of its Founder, Ms. N S Nappinai in collaboration with Red Dot Foundation, of Ms. ElsaMarie D'Silva, its Founder / Director, the **"Cybercrime Awareness through Gender Lens"** awareness program, addressed the following:

1. Understanding the different forms of gender bias and gender stereotypes;
2. Challenging gender norms and stereotypes that socially condition women/girls to be subservient
3. How these gender norms and stereotypes influence our behavior on the online space;
4. The various vulnerabilities and forms of online violence and offences specifically affecting women, children and young adults
5. Remedies and legal records available in law for victims of such cyber offences and how to be peer mentor or a support to victims of such cyber offences.
6. The awareness session were conducted not only for children and young adults but also for teachers , faculty members and parents of the participants;
7. The awareness session also included interactive elements including, Questionnaires, Question and Answer Discussion Sessions and Polls during the session for gaining insight into participant awareness levels.

The details of the awareness programs conducted are as below:

Cyber Saathi online sessions:

Period of Sessions	Number of Sessions	Number of Students	Number of Faculty	Number of Parents	Total number of participants
July, 2020 to -September, 2020	10	1206	52	92	**1350**

From the data collated from participants during the "Cyber Saathi – Cybercrime awareness through Gender Lens" awareness session in collaboration with Red Dot Foundation, from participants surveyed among different schools reported the following:

1. They had limited awareness and knowledge of cyber laws, cybercrimes, and cyber safety practices.

2. Almost all the respondents also reported that it is difficult for a victim of cybercrime to seek legal remedies in India.

3. Responses to survey questions and Polls indicated the importance of discussing gender inequality amongst students in education as well as addressing the issue of gender inequality.

4. Additionally, data collected from students, teachers, and parents during the "Cyber Saathi – Cybercrime awareness through Gender Lens":

a. From **Green Meadows School in Goa** showed that among the 54 participants surveyed, 89% reported that children are more likely to experience cybercrimes, 80% reported that children are more susceptible to crimes related to cyberbullying and 65% of the students reported that they would feel confident in reporting a crime. 52% of parents and teachers reported that social media influences the behaviour of children and youngsters, 87% stated that children and youngsters do not have adequate knowledge of their rights about cybercrimes.

b. Data collected from 87 students, teachers, and parents from **Heritage Girls School, Udaipur** showed that 71% claimed children are more likely to be victims of cybercrimes, 76% reported that cyberbullying is more prevalent in children and only 47% of participants felt confident in reporting a crime.

c. Only 14% of participants stated that they have adequate knowledge of their rights about cybercrimes. Thus, the school curriculum needs to address all facets of cyberbullying as well as gender sensitivity; emerging cybercrime issues must be initiated by the education system.

Some gender targeted cybercrime offences discussed during the "Cybercrime Awareness through Gender Lens" awareness sessions as well as remedies available to victims:

In many cases, victims of a cybercrime are often deterred from reporting a crime due to their lack of awareness, or the societal stigma attached to such crimes, including victim shaming and blaming. However, reporting of such crimes are the first steps towards bringing more accountability and creating a safer space online, so that these victims are protected from being further victimized by perpetrators.

It is therefore important to create awareness of the various cyber offences, how users can protect themselves whilst navigating the online space and remedies available in law in the event they do fall prey to perpetrators online. Some of the prevalent cybercrimes affecting children and young adults addressed during the "Cybercrime awareness through Gender Lens" awareness sessions, through case study examples and participant discussions are as below. The awareness sessions not only dealt with the elements of the various offences, but also how the participants could identify them, avoid falling victim to such offences and how to seek legal recourse in the event they fall victim or know someone who is a victim of such offences.

1. Sexist Hate Speech: Online Hate Speech and Sexism has been on the rise in India. The major difference between cyberbullying and hate speech, is that while cyberbullying is directed towards individual people, hate speech is directed towards a class of people, which in case of sexism is usually women. While the Indian Penal Code does not

recognize gender as a ground for hate speech under Section 153A, most social media platforms allow for reporting of such content by users.

2. Cyber Stalking: Cyber Stalking, refers to the use of internet and electronic media, to harass, repeatedly contact someone etc. Section 354D of the Indian Penal Code deals with stalking and includes cyber stalking within its definition. Along with cyber stalking other provisions of law such as obscenity, defamation, outraging modest etc. may also overlap depending on the facts and circumstance of each case. One of the peculiar aspects of Cyber Stalking is that often perpetrators are anonymous. This often leads victims to believe that they cannot report the crime, however the same is untrue and victims can still report such offences. More awareness needs to be created to make victims aware of their rights. Another aspect of cyber stalking, concerning adolescent and young adult perpetrators is that they are often not aware that certain acts done by them amount to a crime. It, therefore, becomes important to sensitize them about their online behaviour as well.

3. Cyber Extortion: Cyber Extortion refers to threatening victims of exposing private information about them. In many cases, victims are threatened and stopped from filing cases and reaching out to law enforcement authorities (e.g., Shakti Mills Case). Perpetrators behind such a crime, often rely on the vulnerabilities of the victims and use that to threaten them. Provisions such as 66, 67, 67A of the Information Technology Act, 2000 can be relied upon. The Supreme Court in the case of *'Re: Prajwala Letter Dated 18.2.2015 Videos of Violence Against Women & Recommendations' (Suo Motu Criminal Writ Petition No.3 of 2015)* is looking at various technological measures to block uploading of any obscene content at source including exploring the possibility of use of Artificial Intelligence enabled tools to root out these heinous crimes from online platforms. Some such directions have already been issued for limiting the harm caused by these forms of offences as the law provides ZERO TOLERANCE for such offences against Children.

4. Cyberbullying: Although cyber bullying is not explicitly defined under any Indian laws, there exist several provisions like Section 507, Section 354 etc. of the Indian Penal Code, 1860 and Section 67/67A of the Information Technology Act, 2000 (Amended) which can be relied upon, depending on the facts and circumstances of each case. Cyber Bullying can affect all genders, but it has been evident from recent reports, including by the National Commission of Women that women and children are more likely to face bullying because of their gender, perceived weakness and existing social inequalities. The problem of gendered targeted cyberbullying, especially against women and children belonging to a marginalized community, becomes more aggravated as, these sections of society do not always have the access and resource to seek help and avail of remedies

available in law. Caste, class, sexual orientation, religion etc. of women are additional factors that contribute towards cyber bullying.

5. Aside from the above legal remedies available to victims, the awareness sessions also addressed the following important issues and concerns that participants had:

    a. Content that may have been saved in multiple devices can be tracked and more importantly upload of identified content can be blocked.
    b. All of this will be feasible only if you take the help of law enforcement.

Some of the outcomes / feedback that we received from the participants as well as the schools / colleges:

1. Increased knowledge on digital rights and gender equality.

2. Increased confidence in seeking remedies and legal recourse due to the awareness and knowledge of the remedies available in law.

3. Awareness, understanding and access to information on various gender issues and cybercrime and remedies available, so that the participants can act as peer mentors who can be first level responders to help assist other victims of such offences;

4. That the session threw light on gender discrimination, especially of women, in all spheres, in the physical space and how such gender discrimination is transposed to the online space.

5. The session also drew attention to how such gender discrimination and stereotypes result in various cyber offences against women and young adults;

6. That the session were interactive with discussions, polls and questionnaires interspersed during the session which not only kept participants involved but also gave insight into the view points of the other participants

7. The Question & Answer round during the session also helped the participants address any specific queries or concerns they had.

8. Participants also had the opportunity to share their experiences which enabled other participants to relate their own experiences.

9. The availability of the option for filing of online complaints for cybercrime offences through www.cybercrime.gov.in website set up by the Ministry of Home Affairs which provides victims with easy access to immediate legal recourse

10. The sessions gave the participants a better understanding of the various elements and components of cyber offences

The first step in resolving the problem of increasing cybercrimes, particularly in the gendered context in the time of the pandemic is

- Acknowledgement of the problem.
- Creating awareness about the various vulnerabilities in the online space,
- Creating awareness of how users can identify potential threats and
- Remedies available to them in the event they fall victim to such cyber offences.

Vulnerable groups should be made aware of all types of cybercrimes and how to handle them, particularly women, girls, children, elderly people, etc. Spreading adequate understanding of the safety tips of internet usage is vital

It is also therefore important that all Educational institutions encourage students to be responsible users of the internet by incorporating Cybercrime awareness programs as part of their curriculum. This Cybercrime awareness curriculum should not only be extended to students but also to parents, teachers and faculty of schools and colleges.

It is therefore the need of the hour for victims, through awareness and knowledge of the various cybercrimes and legal remedies available to adopt effective and preventive steps to deter and control cybercrime, such as seeking appropriate responses to deal with a harasser, contacting the police, and filing complaints.

It is also important for children and young adults be aware of the personal and sensitive information they are sharing on social media. Preventing disclosure of any personal information or photographs to strangers via e-mail or when communicating online, Stopping all contact and correspondence with the person persistently stalking or bullying through reporting or blocking, but retaining any evidence of stalking (such as voicemails, texts, emails, etc.) for potential court proceedings or criminal actions, talking to family and friends about the abuse to avoid distress or contacting a specialist victim support charity to obtain professional emotional support.

Trivialising, normalising and failing to treat this online malaise have intensified and amplified online misogyny and anti-feminism narratives online to heightened levels of toxicity, that cause harms equivalent to or of much higher impact those resulting from physical violence. (Nappinai N.S., 2020)

In a society, crime occurs due to the prevalence of numerous personal, economic, political, and social factors. Complete elimination of cybercrime is not the purpose of the system for

prevention, but a step towards discussing and attempting to minimise crime and increase awareness.

****

Glossary

Defamation: publishing of defamatory information about the person and distributing it among the victim's social group.

Denigration: the process of making derogatory comments about the target and publishing them online.

Doxing: publishing sexually implicit images or videos against a particular individual to invite internet antagonists to search targets in 'real' life.

Email spoofing: the act of sending a fake or fraudulent email to the victim. This email has pretentious information about the sender, leading the victim to believe that the email was created from another source.

Exclusion: the deliberate refusal to accept a friend on a social networking site.

Flaming: intense online interactions involving insults, offensiveness, unsympathetic tone, uninhibited language, and sarcasm.

Ghosting: abruptly ending all means of contact with a conversation partner without notice or explanation.

Masquerading: the use of the name or likeness of another person without their permission.

Morphing: editing the original picture with a false or unauthorised identity. Cybercriminals download photos of the victims (from social networking sites, etc.) and upload them again after morphing them.

Outing: the public display, uploading or sharing of personal communication or pictures, in particular communication involving confidential personal information or images of a sexual nature.

Phishing: the attempt of gaining sensitive information of the victim such as username and password.

Revenge porn: the non-consensual publishing of sexually implicit images or videos against a particular individual without their consent.

Sextortion: blackmailing and threatening victims online to perform sexual activities.

Trickery: tricking or manipulating others to disclose secrets or embarrassing information, which is then shared online.

Trolling: the malicious provocation of others using manipulation and harmful behaviour on the internet for enjoyment.

References

(2018) 17 SCC 79: In Re: *Prajwala Letter Dated 18.2.2015 Videos of Violence Against Women & Recommendations'* (Suo Motu Criminal Writ Petition No.3 of 2015).

Aggarwal, G. (2015). General awareness on cyber crime. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(8), 204-206.

Agrawal, S. (2020). Online sextortion. *Indian Journal of Health*, *6*(1).

Arpana, M., Chauhan, M., & GJIMT, P. I. (2012). Preventing cyber crime: A study regarding awareness of cyber crime in tricity. *International Journal of Enterprise Computing and Business Systems*, *2*(1), 1-10.

Bannink, R., Broeren, S., van de Looij–Jansen, P. M., de Waart, F. G., & Raat, H. (2014). Cyber and traditional bullying victimization as a risk factor for mental health problems and suicidal ideation in adolescents. *PloS one*, *9*(4), e94026.

Bhattacharyya, R. (2019). Sexual harassment In Company: India inc Reports 14% rise in sexual harassment complaints in FY19. Retrieved from https://economictimes.indiatimes.com/news/company/corporate-trends/india-inc-reports-14-rise-in-sexual-harassment-complaints-in-fy19/articleshow/71288712.cms?frommdr

Blackwell, L., Dimond, J., Schoenebeck, S., & Lampe, C. (2017). Classification and its consequences for online harassment: Design insights from heartmob. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW), 1-19.

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest L. Rev.*, *49*, 345.

Child Relief & You ('CRY') 2020 Report: 'Online Safety & Internet Addiction'. *Available at:*
https://www.cry.org/wp-content/uploads/2020/02/Online-Safety-and-Internet-Addiction-p.pdf.

Cyber Saathi (2020). Case Studies on various forms of cybercrimes. Available at: https://www.cybersaathi.org/case-studies/.

Duggan, M. (2017). *Online Harassment 2017*. Pew Research Center: Internet, Science & Tech. Retrieved from https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

ETGovernment. (2020). Lockdown: Working women complain of 'online' sexual harassment, say experts - et government. Retrieved from https://government.economictimes.indiatimes.com/news/digital-india/lockdown-working-women-complain-of-online-sexual-harassment-say-experts/76150527

European Union Parliament's 2018 Study: 'Cyber violence and hate speech online against women'. *Available at:* https://op.europa.eu/en/publication-detail/-/publication/1ccedce6-c5ed-11e8-9424-01aa75ed71a1;

Gupta, T., Swami, M. K., & Nebhinani, N. (2020). Risk of digital addiction among children and adolescents during COVID-19 pandemic: Concerns, caution, and way out. *Journal of Indian Association for Child & Adolescent Mental Health, 16*(3), 199–208.

Halder, D., & Jaishankar, K. (2012). Cyber Victimization of Women and Cyber Laws in India. In *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 742-756). IGI Global.

Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. *Journal of politeness research*, *6*(2), 215-242.

Hase, C. N., Goldberg, S. B., Smith, D., Stuck, A., & Campain, J. (2015). Impacts of traditional bullying and cyberbullying on the mental health of middle school and high school students. *Psychology in the Schools*, *52*(6), 607-617.

Hatchimonji, J. S., Swendiman, R. A., Seamon, M. J., & Nance, M. L. (2020). Trauma does not quarantine: Violence during the COVID-19 pandemic. *Annals of surgery*, *272*(2), e53.

Human Rights Watch (HRW). (2017). 'Everyone blames me': Barriers to justice and support services for sexual assault survivors in India. United States of America: Human Rights Watch. Retrieved from https://www.hrw.org/sites/default/files/report_pdf/india1117_web.pdf

India Child Protection Fund, April 2020, Child Sexual Abuse Material in India: Report on Demand for Child Pornography & Pilot Deterrence using Artificial Intelligence (https://7d53df5d-623a-479f-89b5-c88a0757a721.filesusr.com/ugd/aeb656).

John, M. E. (2020). Feminism, sexual violence and the times of# MeToo in India. *Asian Journal of Women's Studies*, *26*(2), 137-158.

Kaur, R. (2015). Cyber Crime Against Women-Present Scenario. *International Journal in Management & Social Science*, *3*(9), 223-241.

Kumar (2018). More workplace harassment PLAINTS from public Sector: Bengaluru news - times of India. Retrieved from https://timesofindia.indiatimes.com/city/bengaluru/more-workplace-harassment-plaints-from-public-sector/articleshow/67307053.cms

Li, Q. (2007). Bullying in the new playground: Research into cyberbullying and cyber victimisation. *Australasian Journal of Educational Technology*, *23*(4).

Madaan, N, (2020). Pune: Cybercrime complaints go PAST 2019 tally in 8 months: Pune news - times of India. Retrieved from https://timesofindia.indiatimes.com/city/pune/cybercrime-complaints-go-past-2019-tally-in-8-months/articleshow/77643486.cms

Mehta, S., & Singh, V. (2013). A study of awareness about Cyber Laws in the Indian Society. *International Journal of Computing and Business Research*, *4*(1), 1-8.

Mirchandani, M. (2020). *Tackling Insurgent Ideologies in a Pandemic World* (p. 59). New Delhi: Global Policy.

Mittal, S., & Singh, A. (2014). A study of cyber crime and perpetration of cyber crime in India. *Cyber Law, Privacy, and Security,* 1080-1096.

Mokha, A. K. (2017). A Study on Awareness of Cyber Crime and Security. *Research Journal of Humanities and Social Sciences*, *8*(4), 459-464.

Muzamil, M., & Shah, G. (2016). Cyberbullying and self-perceptions of students associated with their academic performance. *International Journal of Education and Development using ICT*, *12*(3).

Nappinai. N. S. (2017). “Technology Laws Decoded”. Lexis Nexis.

Nappinai N. S. (2020). “Gendered Hate Speech & Crimes Online: Why We Need More Effective Enforcement”. Shethepeople.tv. *Available at*:

https://www.shethepeople.tv/home-top-video/gendered-hate-speech-crimes-online-effective-enforcement-n-s-nappinai/.

Nappinai N. S. 2020, “Separate Laws for Separate Offences – Cyber Bullying & Defamation Online” – (https://www.shethepeople.tv/home-top-video/separate-laws-separate-offences-cyber-bullying-defamation-online-ns-nappinai/)

Nappinai. N. S. (2021). “Role of Law in Combatting Online Misogyny, Hate Speech and Violence Against Women and Girls”. ITforChange.net. *Available at: https://itforchange.net/sites/default/files/1883/NS-Nappinai-Rethinking-Legal-Institutional-Approaches-To-Sexist-Hate-Speech-ITfC-IT-for-Change.pdf;*

Nappinai. N. S. (2021). Cybercrimes & Cybersecurity Laws for India – A Complete Overhaul or Revisiting Existing Legal Framework. Cybersaathi.org. (https://www.cybersaathi.org/research-papers-reports/).

Narahari, A. C., & Shah, V. (2016). Cyber Crime and Security–A Study on Awareness among Young Netizens of Anand (Gujarat State, India).

National Crime Records Bureau - Government Agency (https://ncrb.gov.in/).

Oshima, N., Nishida, A., Shimodera, S., Tochigi, M., Ando, S., Yamasaki, S., ... & Sasaki, T. (2012). The suicidal feelings, self-injury, and mobile phone use after lights out in adolescents. *Journal of pediatric psychology*, *37*(9), 1023-1030.

Patel, A. B. (2015). Crime against the women in India. *Foresic Research & Criminology International Journal, 1*(4).

Poulpunitha S., Manimekalai K., Veeramani, P. (2020). Strategies to prevent and control of CYBERCRIME against women and girls. *International Journal of Innovative Technology and Exploring Engineering, 9*(3), 609-612.

Rao, T. S., Bansal, D., & Chandran, S. (2018). Cyberbullying: A virtual offense with real consequences. *Indian journal of psychiatry*, *60*(1), 3.

Reuters (2018). Exclusive: India most dangerous country for women with sexual VIOLENCE rife - global poll. Retrieved from https://www.reuters.com/article/us-women-dangerous-poll-exclusive-idUSKBN1JM01X

Sarkar, B. (2019). More than 50% women professionals believe sexual harassment at the workplace has increased over the years: Survey. Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/more-than-50-women-prof

essionals-believe-sexual-harassment-at-the-workplace-has-increased-over-the-years-survey/articleshow/69855500.cms?from=mdr

Schoffstall, C. L., & Cohen, R. (2011). Cyber aggression: The relation between online offenders and offline social competence. *Social Development*, *20*(3), 587-604.

Shivashankar, B.S., & Prakash, A. (2018). A Critical Analysis of Cyber Bullying in India-with Special Reference to Bullying in College. *International Journal of Pure and Applied Mathematics, 2018.* Retrieved from https://ssrn.com/abstract=3554114

Sharma, A. (2020). Online sexual harassment: A legal insight for working women. Retrieved from https://www.peoplematters.in/article/life-at-work/online-sexual-harassment-a-legal-insight-for-working-women-27108

Spend, I. (2017). Despite law, 70% working women do not REPORT workplace sexual Harassment; Employers show poor compliance. Retrieved from https://www.indiaspend.com/despite-law-70-working-women-do-not-report-workplace-sexual-harassment-employers-show-poor-compliance-94743

The Hindu, 2020, "Coronavirus lockdown: Govt. helpline receives 92,000 calls on child abuse and violence in 11 days" from

(https://www.thehindu.com/news/national/coronavirus-lockdown-govt-helpline-receives-92000-calls-on-child-abuse-and-violence-in-11-days/article31287468.ece)

The New Indian Express. (2020). 'Significant' increase in cybercrime against women during lockdown: Experts. Retrieved from https://www.newindianexpress.com/nation/2020/may/01/significant-increase-in-cybercrime-against-women-during-lockdown-experts-2137987.html

****