VOLUME 20 ISSN 2456-9704

RISING CRIME AGAINST WOMEN & CHILDREN IN CYBERSPACE: A CONCERN

By Sahil Goel
From Amity Law School, Noida

Chapter 1

Abstract

Cyber space refers to facility or feature which involves internet. This includes virtual world of computers which allow users to share information, interact with each other, swap ideas, engage in discussions, create initiative media, social forums & many other activities. Unfortunately, this cyber space has also become a medium of crime against women which is referred to as "Cyber Crime" in common parlance. While the world has witnessed a digital revolution, at the same time it has provided an entry for such people who tend to exploit such revolution.

It is impacting a huge no. of population including men, women & youth in the working class. The question here is that, Why social media today has become a platform for those who tend to take undue advantage of this to harass and abuse women & girls for their curious pleasures like stalking, bullying, violation of privacy, abusing etc with the help of inappropriate means. Why always women become victims? Just because they are considered to be emotionally weak and unstable in society? Why are the perpetrators able to take undue advantage of those considered relatively weaker in society through the means of technology? While the technology is supposed to strengthen the masses, the perpetrators still use it as a way to overpower the sections of society such as women. Why has the technology been used in wrong direction to take advantage of the lacunae in law & commit crime. Why child pornography has reached today at an alarming level worldwide? Why are the women not able to equate themselves to other sections of society despite having the provisions of a governing law in place? How capable are our agencies in prosecuting cybercrime?

It is high time to take strong steps to strengthen the cyber law and also put legislations into place that could curb such activities. It is because of the lacuna in law that people have strong courage to indulge in such activities. Its the responsibility of the state to eliminate the flaws in law in order to prevent crime against women in digital world. We need to create awareness to the weaker sections of the society as well against such crimes and also strengthen the laws for the intermediary liability in the digital world so that a deterrent effect can be created for such perpetrators.

Keywords: cyber space, cyber crime , weaker sections. Inappropriate content, perpetrators, deterrent liability

Introduction

The internet has been one of the greatest creations in the field of correspondence. [1]New communication systems & digital technology have made dramatic changes in the way we live. [2]With the advent of internet, the whole world has become a global village.

[1] Rohas Nagpal, Ecommerce Legal issues 6 Asian School of Cyber Laws, Pune, 2019

[2] http://www.cybercrimejournal.com/sahasrivastavatalijcc2014vol8issue1.pdf

It has created a virtual world with no boundaries, which gives people ample opportunities to ameliorate both personal and professional relationships across borders. Cyber-crime is broadly used to describe the activities in which computers or networks are a tool, a target, or a place for criminal activity.

[3]A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit material in electronic form, video voyeurism and breach of confidentially and leakage of data by intermediary, ecommerce frauds like personation commonly known as phishing, identity theft & offensive messages through communication services.
[4]Since this technology has no physical limits; it streams effectively around the globe. As a result, the place where cyber crooks commit crime & where its effects are produced is totally different & cyberspace is no special case to it. Thus, cybercrimes against women are on the rise & women & children have been radically victimized in the cyberspace. Cybercrime is a worldwide phenomenon & women & children have become the vulnerable objectives of this new type of wrongdoing.
Despite the fact that India is one of the very few nations to enact the IT Act 2000 in order to battle crimes in cyberspace, issues with respect to women have not been given attention to in this Act. The said Act has named certain offences like hacking, publishing of obscene content in the cybersapce, fiddling with the data as culpable offences. But the grave risk to the security of women isn't covered completely by this Act.

At the point when India began its journey in the field of Information Technology, attention was given to protect electronic commerce transactions & communications under Information Technology Act, 2000 while issues like safety of women in cyberspace, provisions relating to image morphing, cyber defamation etc were not paid heed to. Since social media had not developed at that time, so provisions relating to crime against women & children on social media were not added in the Act. Since, in 2000, technology was very different, intermediaries were only considered to that who provided bandwidths, gave connections etc. Today the concept of intermediary has totally changed. Social networking sites have today become a new tool for the perpetrators to commit various types of crime as women & children spend long hours on it for entertainment, establishing online relationship with strangers whom they call as virtual friends who then become the reasons for they getting victimized. It is apparent that threats of rape and sexual violence are used to intimidate victims *via* social media. Cloned profiles or fake profiles of female victims are created by stealing the personal information from the social media profiles of the female member or by hacking their systems.

According to a Research based study, 1 in 3 internet users worldwide is a child & 7,50,000 individuals at any point in time are estimated to be looking to connect with

[3] Rohas Nagpal, Ecommerce Legal issues 9 Asian School of Cyber Laws, Pune, 2019

[4] http://www.cybercrimejournal.com/sahasrivastavatalijcc2014vol8issue1.pdf

children for sexual purposes. [5]Also according to a data of 2017 released by National Crime Records Bureau (NCRB) in October, 2019 it was shocking to know that cybercrimes almost doubled in India in 2017 with figures reaching to 21,796 cases out of which 1460 cases were related to sexual explitation & in [6]2018 total reported cases of cybercrime by NCRB were 27248 which is an alarming situation.

-
- **Review of literature**

The world in 2020 has witnessed a covid-19 pandemic. Covid-19 has proved to be a gold mine for cybercriminals. [7]According to an antivrus company Quickheal, it detected 50,000 malicious URLs & 40,000 malwares hiding behind information about the pandemic. India has already witnessed an 86% rise in cybercrime post covid-19 pandemic. This is due to the fact that there has been a significant rise in internet traffic due to the lockdown & perpetrators have exploited the situation by creating fake sites, sending malicious links in the name of providing services such as offering great discounts on medicines required for the treatment of corona virus. Since women & children are unaware of this, they become victims of such practices & end up getting blackmailed to reveal their personal information or their system getting hacked without they getting to know the same.

Cybercriminals are quite aware of the fact that its very difficult for the women & children to report the crime to the nearest police stations as police too would be busy in managing the covid-19 lockdown situation which became the major reason for rise in such crimes during covid-19 lockdown period. Such crime goes unreported as Indian women & children are unaware of such offences.

[8]Google blocked 18 million fake ads (bad ads) daily & 240 email messages that were spam amid the COVID-19 lockdown during lockdown in the month of April, to stop phishing attacks on women & children & prevent cheating by personation. Barracuda, an IT security company has also seen a 667% spike in spear phishing attacks happening post covid-19 lockdown. This increasing rate of cyber-crime against women & children has led to development of insecurity among them. They don't feel safe anymore, anywhere. Its effects are worse on them and on the society as a whole, when we look into the broader picture.

The research for the sake of understanding has been broadly divided under the various chapters. Firstly, various types of crimes in cyberspace have been discussed along with some case studies. Secondly, the reasons for growth in crime against women in cyber space have been discussed. This part of the

5 https://www.google.co.in/amp/s/www.livemint.com/v/s/www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017/amp-11571735243602.html%3fusqp=mq331AQFKAGwASA%253D&_js_v=0.1#ampf=

6 https://www.newindianexpress.com/nation/2020/feb/23/india-stands-third-among-top-20-cyber-crime-victims-says-fbi-report-2107309.html

7 https://www.linkedin.com/feed/news/scamsters-make-hay-amid-pandemic-5165994/

8 https://www.businessinsider.in/tech/news/google-blocked-an-average-of-18-million-daily-malicious-coronavirus-messages-to-gmail-users-in-the-past-week-as-hackers-try-to-capitalize-on-fear-and-less-secure-remote-work-setups/articleshow/75205021.cms

study covers that why women & children have become vulnerable objects in cyberspace. Thirdly, the steps taken by the Indian government in recent years to curb & prevent crime against women in cyber space along with the reporting mechanism of cybercrime has been discussed. Fourthly, crimes against children have been discussed. Fifthly, global action taken by agencies i.e. Interpol & virtual global taskforce (VGT) to control & reduce child pornography worldwide has been discussed. In the last impact of COVID-19 on economy with special emphasis on cyber world has been discussed along with some suggestions & conclusion.

Chapter 2

Types of crime against women in cyber space

In India crime against women in cyber space" includes sexual crimes, sexual abuses on the internet & crimes on social media. Majority of the cases relating to crime against women in cyberspace which are reported to the police come within the scope of Section 67 (Publishing or transmitting obscene material in electronic form) of the IT Act, 2000. Perpetrators who are males, mostly commit cybercrime for sexual purposes like morphing, using the picture for the purpose of pornography, cyber stalking etc & nonsexual purposes i.e. Harassing or bullying the victim. Perpetrators who are females commit such crime mostly for ideological differences, hatred or to take revenge.

Women in cyberspace are victimized in the following ways by the perpetrators.

Cyber Stalking/Cyber Bullying- It is one of the most popular crimes in the digital world. [9]An individual may stalk or harass an individual, group, or organization through internet. A cyber stalker may follow a person's movements across the Internet by posting messages to threaten the victim on the bulletin board accessed by him, entering the chatrooms used by the victim or by continuously sending emails, instant messaging to the victim.

[10]The perpetrators basically involve in cyberstalking for sexually harassing the victim, the perpetrator being obsessed by victims love, taking revenge for some past insult by the victim or due to a feeling of grudge towards the victim. A stalker may harass his targets via private emails or sending message publicly. Women especially of the age group of 16 to 35 become the victims for most of the cyber stalking cases. Such acts can make a stalker liable for 3 years imprisonment under sec-354-D of the Indian Penal Code.

Morphing: [11]Its an activity to edit original picture to misuse it. Preparators download women pictures from social media i.e facebook, instagram etc or some other resources & use the morphed photos for creating fake profiles on social networking sites or any pornographic sites which also becomes the case of cheating by personation which could make a person liable for 3 years of imprisonment alongwith a fine of 1 lakh rupees under sec-66D of the IT Act,2000.

[9] https://en.wikipedia.org/wiki/Cyberstalking

[10] https://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf

[11] https://acadpubl.eu/hub/2018-118-21/articles/21b/68.pdf

Cyber defamation- [12]It involves defaming a person through a new and far more effective method such as the use of modern Electronic devices. It refers to the publishing of defamatory material against any person in cyberspace with the help of computers or the Internet which could include defaming stories against the victim. If an individual engages himself in publishing any kind of defamatory statement against any other individual on a website or sends E-mails which contains defamatory material to that individual to whom the statement has been made would lead to Cyber defamation. Unfortunately, cyber defamation has not been defined in the IT Act, 2000 due to which perpetrators take advantage.

Cyber pornography -[13]It can be defined as an obscene material designed, published or distributed using cyber space as a medium. In India, if an individual watches pornography, it is not a crime, but if he creates & distributes such content, then it would be a crime. Though, child pornography is not legal in any form & is prohibited globally. It could make a person liable for 5 years imprisonment along with 10 lakh Rupees fine on 1st conviction & 7 years imprisonment along with a fine of 10 lakh Rupees on subsequent conviction under Sec-67A of the IT Act,2000

Hacking- [14]It means unauthorized access to computer system or network, and it is the most predominant form of cybercrime. It is an invasion into the privacy of data, it mostly happens in a social online community to harass a woman by changing her whole profile into an indecent, derogatory one. The reasons could vary from personal grudge, taking revenge or even for fun. 90% of hacks happen through emails or social media accounts, the hacker sends some malicious links & gains access.

Hacking can be done by criminal hiding behind a trustworthy entity for acquiring sensitive information (Phishing), infecting a website by malware usually visited by the victim (Watering Hole Attack), or by installing rootkits, keystroke loggers, ransomwares etc

Email spoofing-[15] It is the falsification of an email sender address with the goal that the message seems to have originated from somebody other than the real source.

Vishing- It is telephone equivalent of phishing. The perpetrator may use the telephone & pretend to be a legitimate entity in order to scam the victim into surrendering private information which he would later use for identity theft in the cyberspace.

Cases laws:-

Ritu Kohli Case, 2000

[16]This was the 1st case of cyberstalking in India. Manish Kathuria stalked an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, www.mirc.com using her name.

---

12 https://blog.ipleaders.in/cyber-defamation-india-issues/

13 https://www.digital4n6journal.com/cyber-pornography/

14 https://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf

15 https://www.agari.com/email-security-blog/what-is-email-spoofing/

16 http://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf

He used indescent & obnoxious language, & shared her home telephone number to invite people to chat with her on the phone. As a result, Ms. Ritu Kohli received calls from various states of India & abroad, people conversed badly with her. The police registered her case under sec 509 (outraging the modesty of women), IPC. But the section was silent for outraging the modesty of women on the web. This raised a concern to the government, for amending the laws regarding the aforesaid crime & protection of victims in the cyber space. Many such cases were reported, where the accused could not be convicted due to the IT Act, being silent on such issues.

As a result, the IT Act, was amended in 2009 , wherein sec-66A was inserted which provided for an imprisonment for up to 3 years along with a fine, if a person was held guilty of sending offensive messages or false information in order to annoy or insult the person to whom such message was sent. But the section was struck down in 2015 by the Supreme Court of India in the [17]Shreya Singhal case.

Why Sec-66A was declared as unconstitutional?

The Supreme court of India in Shreya Singhal case, declared section 66A of the IT Act, as unconstitutional, being violative of freedom of speech & expression under Article 19 (1)(a) of the Constitution of India. Section 66A of the IT Act, was debated & in controversy mainly because it was seen as being against freedom of speech as it used vague words like grossly offensive, menacing character etc. [18]In the last few years, this section was used in many controversial cases including the arrest of chemistry professor at Jadavpur University just because he forwarded a cartoon featuring the West Bengal CM Mamata Banerjee. A month later two Air India cabin crew members were arrested & jailed for 12 days as they posted derogatory remarks against the Prime Minister's office, the national flag & the Supreme Court while commenting on a strike by Air India's pilots.

Later that year, two girls got arrested over a Facebook post which questioned the shutdown in Mumbai for Shive Sena patriarch Bal Thackeray's funeral. That arrest led to a nation-wide protest & prompted a law student to file a public interest litigation challenging the constitutional validity of section 66A. [19]On 9th January, 2013, the Central Government issued an advisory that if a person got arrested under section 66A, it must be first approved by an officer of the rank of the Inspector General, Deputy Commissioner or Superintendent of Police. On 24th March, 2015, the Supreme Court in a 122-page judgement, struck down section 66A in its entirety for violating the fundamental right of speech & expression.

[20]**SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra,**

This was the 1st reported case of cyber defamation in India. [21]It was contended by the plaintiff that the defendant was sending

[17] Shreya Singhal vs UOI, Writ Petition (Criminal) 2012 SC 167

[18] Rohas Nagpal, Cyber Crime Law in India 89 Asian School of Cyber Laws, Pune, 2019

[19] Rohas Nagpal, Cyber Crime Law in India 90 Asian School of Cyber Laws, Pune, 2019

[20] 65/14, Original Suit No. 1279 of 2001, District Court, Delhi

[21] https://www.legalserviceindia.com/lawforum/cyber-laws/17/smc-pneumatics-v-jogesh-kwatra-indias-first-case-of-cyber-defamation-case/2240/

emails to the plaintiff & its subsidaries that were defamatory, abusive, obscene, vulgar with an aim to malign the high reputation of the plaintiff & its Managing Director all over India and the world. The defendant being an employee of the plaintiff was under a duty not to send the aforesaid emails. The Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails and passed an important ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries & also restrained the defendant from publishing, transmitting etc any information in cyberspace which is derogatory or defamatory of the plaintiffs.

[22]DPS MMS Scandal Case

[23]In this case an obscene video by the title- "DPS girl having fun" was uploaded under the category of "ebooks" (to avoid falling under any filter by the site) by an IIT Kharagpur student who was one of the sellers on an ecommerce site www.bazee.com & was successful in selling some copies of the MMS clip. As a result, the CEO of bazee.com, Mr. Avnish Bajaj was arrested under sec-67 for distribution of cyber pornography through the site. Since no prime facie evidence could be found that Mr. Bajaj was directly or indirectly involved in publishing the pornography as the video could not be seen on the site due to remedial measures taken by the back end team, he was realeased on bail. This case raised questions regarding efficiency of the IT Act, & raised a need to amend it. As a result, intermediary guidelines were passed in 2011 which stated that if an intermediary had exercised due diligence to remove obscene material on their content, then they can escape liability.

Chapter 3

Reasons for growth of crime against women & children in cyber space

The main reason for growth of crime against women in cyber space is that its of transcendental nature having no boundaries, its dynamic nature, easy access & anonymity due to which perpetrators take advantage. Even if the place from which the crime has taken place is detected, it sometimes becomes very difficult for the police to catch hold of the perpetrators. While there are many other reasons for rise of cybercrime against women which have been discussed as under-

●**Legal Reason-** From the preamble of the IT Act, 2000 it can be clearly inferred that the intention of the legislature to enact the Act in 2000 was to give legal recognition to the transaction taking place by "electronic data interchange" & over ecommerce & hence it focused mainly on provisions relating to unauthorized access, breach of confidentiality etc. Most of the crimes in cyber space are prosecuted under mainly 3 sections of the IT Act, sec 66 (Hacking), 67 (Publication & transmission of obscene material) & 72 (breach of confidentiality). For crimes like cyber defamation, image morphing, creating fake profiles of women & children on social media etc, the IT Act, is silent which becomes the cause for rise of such crimes.

[22] Avnish Bajaj vs. State (N.C.T) of Delhi [(2005)3CompLJ364(Del), 116(2005)DLT427,2005(79)DRJ576)

[23] Rohas Nagpal, Cyber Crime Law in India 119 Asian School of Cyber Laws, Pune, 2019

●**Sociological Reason-** India witnesses a patriarchal system of society where males are considered to be bold & tough & women are treated as introvert & submissive which becomes a major cause for rise in cybercrime against women. [24]Men attach respectability of a family on the honor of the women members, which makes women vulnerable to perpetrators as sometimes they also change their identity in order to harass or blackmail women in cyberspace. Most of the cybercrimes remain unreported due to the hesitation and shyness of the victim and her fear of defamation of family's name which too is a major reason for rise in.

●**Psychological Reason-** With the birth of nuclear family culture in India, the joint family culture has nearly vanished where people used to share, discuss etc about their lives with family members. The rise of nuclear families have led to people wanting their own privacy & not having time for each other. Due to this women especially homemakers sometimes become targets of depression & loneliness & to overcome this they take support of cyberspace to reach the outside world. When they are unable to reach to close friends or relatives, they land up establishing contact with strangers & giving them information about their family, personal information etc due to which their victimization takes place. Parents have nowadays become impatient due to work stress & they don't have the time to spend time with the family & as a result children especially girl victims are unable to bring such crimes to the notice of parents.
Also when many female students and staff have to live away from family due to job & work for long hours over the computers, it becomes their reliable source as well which too lands them in trouble.

●**Partial Computer Illiteracy-** It has been observed that women have comparatively less knowledge about computers than men which leads to they becoming vulnerable to cybercrimes. Computer literacy just not only includes surfing the net but it is also meant to have good knowledge about computers, such as working of operating systems, its vulnerabilities, privacy protection, protection from computer contaminants such as viruses, worms, Trojans, spyware malware, etc which can lead to breach of security resulting in hacking of the system.
Many a times women are not aware of privacy settings of social networking sites which results in providing easy access to women's personal details, photos etc to the perpetrators & committing such crimes.

●**Other Reasons**
Women sometimes infer that harassment in cyberspace would lead to social harassment as well. As a result of which a woman victim abstains from complaining even if she is victimized because once the crime is reported it is flashed through media or internet, and then it becomes more difficult for the woman to live in the society. She is considered a social stigma by the people.
After the data revolution bought by Reliance Jio in 2016, availability of internet at cheap rates & setting up fake websites through website service providers at an affordable cost has become very common to commit such crimes.

24 http://www.cybercrimejournal.com/sahasrivastavatalijcc2014vol8issue1.pdf

Internet addiction among some children and women for sexual communication & establishing online relationships with strangers in order to relive stress, anxiety, depression, loneliness etc has resulted in increase of such crimes,

Lack of awareness of the types of cybercrimes & its legal implications among many women and children committed against them has given rise to such crimes & perpetrators knowing this fact leads to increase in such cases.

Sometimes the system is incompetent to assist in intercepting, monitoring or decryption which leads to perpetrators being untraced.

Intermediary sometimes fails to block the unwanted content such as fake obscene content etc.

Chapter 4

Recent steps taken by the government to report & curb cyber crime

The government in past few years has taken a number of steps in order to deal with the increasing cybercrime & establish public trust in the digital world. This includes setting up of inter-ministerial committee on phone frauds in 2014. The cybercrime against women & child scheme under which online cybercrime reporting portal has been operationalized.

The Ministry of Home Affairs had constituted an expert group for a detailed study for initiation & creation of a Indian Cybercrime Coordination Center that would holistically deal with cyber forensics, investigation, research and innovation, threat analytics & cyber training.

Accordingly in February 2019, the Ministry of Home Affairs launched the cybercrime investigation center known as the Indian Cybercrime Investigation Center in short for I4C scheme under which a no. of institutions were established including the national cyber forensic lab and the CYPAD under Delhi police which is short for cyber prevention awareness and detention center. [25]Under I4C, following verticals have been established.

1. **National cybercrime threat Analytics Unit (TAU)-**For providing a platform for personnel to implement the law, people from private sector, research scholars to work cooperatively to analyze all bits of cybercrimes.
2. **National cybercrime reporting-** For creating investigation team comprising of experts to work with investigating units that are established at state & central level.
3. **Platform for joint cybercrime investigation team-** For driving action with coordination to combat key threats in cyberspace.
4. **National cybercrime forensic laboratory ecosystem (NCFL)-** For building up a center to assist the process of investigation. NCFL & related Central Forensic Science Laboratory to be well-prepared & very much staffed so as to analyze & stay aware of new specialized turns of events, utilizing which a totally new sort of cybercrime may have been carried out.
5. **National cybercrime training center-** For training on crimes in cyberspace, its investigation & developing online courses for such training.

[25] https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

6. **Cybercrime ecosystem management unit-** For creating ecosystem that would unite the scholarly community, industry and government to work, explore a cybercrime premise with built up standard working techniques to react & contain the effect of crime in cyberspace.
7. **National Cyber Research & Innovation center-** For tracking rising developments in technology, proactively anticipating potential vulnerabilities, which can be misused by cyber crooks.

According to the Ministry of Home Affairs, education & awareness about cybercrime can help in prevention of such crimes to a significant extent. The ministry has established an online cybercrime reporting portal, www.cybercrime.gov.in, where the crime can be reported online. Also the website displays information details about types of cybercrimes & precautions to be taken to avoid becoming victim on social media, matrimonial sites, job seeking sites etc. At the state level most of the police stations have established a dedicated cyber cell for cybercrime reporting. The victim of cybercrime can immediately report the crime to the nearest police station alongwith necessary evidences such as screenshots, etc.

Cyber dost twitter handle

[26]The Ministry of Home Affairs started a twitter handle called "Cyber Dost" in March 2018, which creates relevant posts on how to prevent & be secure against cyber rime. The handle covers topics such as security measures to be adopted by an individual while using the internet, awareness on identity theft etc.

[27]The twitter handle also advises victims of cybercrimes for registering their complaints on the appropriate channel. An individual can also tweet their inquiry on its feed and get a solution for a right strategy to be followed for taking an action against cybercrime. It also released some safety tips to be followed by people during covid-19 lockdown as people were following work from home culture.

Cyber safe women initiative

"Cyber Safe Women Initiative" is a campaign which was propelled by the gvt. of Maharashtra on 3rd January, 2020 on the birth anniversary of Indian social reformer Savitribai Phule to help women & children so that they can be aware of cyber practices.

Key features of the initiative

Under this initiative, the gvt proposed to organize awareness camps pertaining to cyber security for women & children across the whole state of Maharashtra including every district as internet today especially social media has become a new tool for the perpetrators.

[28]The camps would mainly focus on educating & creating awareness among the women & children about how perpetrators exploit the internet to commit crime in cyberspace, the laws related to cybercrime in India & types of cybercrimes such as cyber stalking, online phishing, image morphing, child pornography, fake sites, cyber defamation, fake profile on social media etc

[26] https://currentaffairs.gktoday.in/cyber-safe-initiative-launched-by-maharashtra-government-012020323198.html

[27] https://news.abplive.com/news/india/coronavirus-in-india-all-you-need-to-know-about-cyber-dost-1195940

[28] https://www.jagranjosh.com/current-affairs/maharashtra-launches-cyber-safe-women-initiative-1578033411-1

so that they are not cheated or sexually exploited in cyberspace.
For awareness camps, participation would be invited from women and children including police representatives, district ministers, government officials, school and college students, NGOs, Anganwadi sevaks & members of the Women's Vigilance Committee.

Chapter 5

Crimes against children in cyberspace

Perpetrators very well know the fact, that its much easier to commit crimes against children than adults in cyberspace as children are always excited to explore new things on internet & can be blackmailed easily, therefore crimes against them are committed in following ways-

Child Pornography- Filming a child using webcams or other digital means while doing sex or digital representation in explicit sexual relationship or photographing any if his/her sexual organs. It involves 3 stages Pornography production in which pornographic images are created by collecting it from old magazines & films, then re-directing & displaying their sexual organs. Then comes Distribution of child pornography which involves publishing it on social media websites, closed social networks etc via internet & the last which is the downloading stage which involves perpetrators obtaining child pornography online. It could make the perpetrator liable for 5 years imprisonment along with a fine of up to 10 lakh rupees on 1st conviction & 7 years imprisonment along with 10 lakh rupees fine on subsequent conviction under sec-67B of the IT Act,2000.

Online Grooming- It can also be termed as webcam blackmail. When a sex offender forms an online relationship of trust with a youngster and deceives or pressures him/her into doing sexual act, it is said to be online grooming. This is the most common form of online child sexual abuse.

Sextortion- [29]It can also be termed as webcam blackmail. It is a part of cyber blackmailing. It occurs when the perpetrators tries to blackmail the victim by sending emails mentioning that they have installed spyware or ransomware into the victims system & filmed them using laptop webcam & would share victims sexually explicit images & videos with his social circle, if the victim doesn't pay him money. According to a study, 78% of reported sextortion cases, the victim was a female b/w 8 & 17 years of age.

Cyber trafficking- When perpetrators make use of cyberspace for recruiting the victims for human trafficking, advertising about services offered by victim, to attract clients is termed as cyber stalking.

Crime through online games- Perpetrators know that children are always excited about new games on the internet, for which they design addictive games & also ask to purchase game currency at a discounted rate. Children failing to anticipate the consequences, end up giving their personal & financial information & as a result become victims of hacking, blackmailing phishing (game controller trying to be a legitimate entity but in reality a criminal) etc

Chapter 6

Global action to reduce & control child pornography

[29] https://www.barracuda.com/glossary/sextortion

Interpol

[30]This is the International Criminal Police Organization headquarted in France which curently has 194 countries as it members including India. INTERPOL allows specialized investigators from member states to share data, through the analysis of digital & audio content of photos & videos. Its strategy is based on identifying victims & save them from sexual exploitation, preventing access to child pornography that is used for sexual exploitation which is available online & preventing perpetrators form travelling to commit their crimes or escaping from legal prosecution. Its specialists can identify victims by analyzing the digital, optical & audio contents of photos to extract evidence & locate victims.Interpol has been able to identify thousands of children & arrest thousands of perpetrators form the start of their photo data base since 2001. Amid the COVID-19 pandemic, it has started an awareness campaign on "COVID-19 cyberthreats"

Virtual global taskforce (VGT)-[31]

This organisation aims to use the support of NGOs to provide a program to coordinate law enforcement operations in international cooperation to monitor child exploiters & to control child sexual crime perpetrators online.

The initiative's strategy is based on 3 axes-

●**To block search results that lead to child abuse-** New algorithms have been implemented to prohibit pornographic images & videos for children by identifying & blocking their digital footprint & by identifying the site that promotes it & the blocking of broadcasts on Google & Microsoft.

●**To identify & delete pornographic content for children-** In order to achieve this, Member states decided to establish national databases & contribute to international systems such as INTERPOL's child pornography database which provides international database of child pornography through which it can combat the spread of this crime. Also, Microsoft, Google & Firefox have agreed to coordinate a mechanism to block these images at the browser level.

●**To chase the perpetrators & enforce the law-** When it comes to child exploitation online, the place to publish child pornography is a crime scene. So laws must be enforced by applying all means of transferring & preserving that content, whether it is peer to peer networks, or what we call it as "deep network. Also specialized working groups have been established to control crimes, identify perpetrators & the identity of victims.

Chapter 7

Impact of covid-19 on economy with special emphasis on cyber world

Initially corona virus began in Wuhan, China & the entire world thought it was a local infection & then it grew to such large proportions that it had to be declared as pandemic by WHO. It is the first virus that we have actually seen in human civilization after the development of the internet. Now covid-19 has been described as an infodemic by WHO (1st epidemic in the information age). While there has been an increase in the number of people going on to the internet & confining themselves in their homes, internet has started witnessing new challenges & approaches. This entire trend has been well

[30] https://www.interpol.int/en

[31] http://virtualglobaltaskforce.com/about/

noticed by cybercriminals & cyber security breachers. It's not surprising that we have started witnessing emerging issues relating to use of cyber space by users in the corona virus age. [32]According to India Ratings & research, it appraises an aggregate income loss of around Rs 97,100 crore for 21 significant states in April alone amid the COVID-19 lockdown as it had slowed down monetary movement in the nation. Though the lockdown has caused revenue loss to both the central and state governments, the actual battle against Covid-19 & the related expenditure is being born by states.

Cyber world post COVID-19

Covid-19 is an unprecedented event in the history of humanity in 21st century. Unfortunately we have also seen a tremendous increase in the distribution of child pornography, in the number of images being shared online & in the level of violence associated with child exploitation & sexual abuse crimes.

[33]India Child Protection Fund (iCPF), reported a 95% rise in child pornographic content utilization ever since the lockdown was imposed. On one side, lockdown tried to make people of India safe but on another hand, it destroyed people's thinking as they were going more towards pornography videos.

It indicates that millions of pedophiles, child rapists, and child pornography addicts have migrated online, making the internet extremely unsafe for children as they can be more vulnerable through educational applications via the internet, to unsafe communication with adults or to determine their personal information. Without stringent action, this could result in a drastic rise in sexual crimes against them. Also, the Rajya Sabha Committee on the issue, has recommended stringent laws for Internet service providers like Jio and Airtel, and platforms like Facebook, Twitter, and Instagram, to hold them accountable for child abuse enabled by these companies.

Therefore, the methodologies relating to managing and taking care of with this whole infodemic has been totally new and noteworthy. Indeed, the internet has been utilized as a great infective instrument to spread a wide range of information relating to coronavirus. This could be authenticated, genuine information or unauthenticated, fabricated information. Users, therefore must know that what new repercussions could the corona virus bring as an infodemic for the society at large.

[34]In addition, we have started witnessing nations of the world marginally coming with innovative mechanisms under the cyberlaw frameworks in order to deal with the containment & bogus info relating to coronavirus. There is an enormous no. of cybercrime & cyber security ramifications that we all must know while dealing with the coronavirus & increased reliance of internet in such circumstances.

[35]It has been accounted for that in the 2 months, when coronavirus started, the no. of

[32] https://www.bloombergquint.com/economy-finance/major-states-may-lose-rs-97100-crore-revenue-in-april-says-india-ratings

[33] https://www.thehindubusinessline.com/info-tech/india-lockdown-online-child-pornography-consumption-spikes-by-in-india-says-icpf/article31337221.ece

[34] https://www.udemy.com/course/cyberlaw-cybercrime-cyber-security-coronavirus-pavan-duggal/

[35] https://www.udemy.com/course/cyberlaw-cybercrime-cyber-security-coronavirus-pavan-duggal/

domains that have been registered on coronavirus related things, have massively increased. More than 4000 domain names have been registered on coronavirus related things. While 3% of these domain names are malicious while another 5% are being treated as suspicious. It has been inferred that registered domain names relating to coronavirus are a way more likely to be more suspicious as compared to other domain names that are being registered at the same time.

Chapter 8

Suggestions

●Social Networking sites like Facebook, instagram should guide users especially women & children to check & update their privacy settings frequently so that only the people whom they know can access their profile to avoid fake profiles, image morphing etc.

●Search engines like Yahoo, google, etc should develop advanced algorithms so that when anyone types "child pornography" of related phrase, the results are filtered & no such type of content is displayed to the user.

●Specific provision relating to sextortion, online grooming, phishing, image morphing, crime through online games should be added in the IT Act.

●A separate chapter for social media should be added in the IT Act, stating the specific crimes that could took place in social media, alongwith rights, duties & liabilities of both the intermediary & the users should be clearly defined.

●Sec-79, of the IT Act, talks about the circumstances in which intermediary can be exempted from liability. It states that if intermediary aids, conspires, abates or induces in commission of any unlawful activity, then it would not be exempted from liability. But too much scope for interpretation has been given to the above 4 words for interpretation by courts & as a result of which advantage can be taken by finding out the loopholes to escape liability by intermediary. Hence these words should be defined clearly alongwith the sections.

Conclusion

Covid-19 will always be a milestone gamechanger in our lives & the world will always be referred to as Before Corona (BC) & After Corona (AC) post the pandemic. Each individual needs to know about the cyberspace challenges and issues that have begun to emerge in the coronavirus age. This would enable people to deal with this in an efficient way & to avoid becoming victims of cybercrime. Parents need to spend more time with children so that children don't hesitate to inform them if they become victims of cybercrime. We also must appreciate the efforts of the police in handling cybercrime & Ministry of Home affairs for taking drastic steps to create awareness for cybercrime among women & children & at the same time establishing efficient mechanisms to report cybercrime in recent years. New legislations will have to be constantly enacted in order to cope up with the rapid changes in technology & newer forms of crimes.

We have seen that cyberlaw is slowly coming to the mainstream & IT Act continues to be a evergreen hero. Countries have now started coming up with new legislations to combat cyber security breachers as cybercrimes have now become a part of our lives.

*****