LEGAL ANALYSIS: CYBERCRIME AND ITS IMPACT ON YOUTH

Naman Jain D.M.E Noida, GGSIPU

ABSTRACT

Human civilization has benefited much from internet. The technology has brought individuals from all over the globe together. The social media platforms have created a new social realm. Computer-based violation is currently a common problem destroying the realm. Our country is moreover not free from its grips. It is a usual danger that is not restricted to any perimeter. It can be held out from anywhere in the realm as well as contrarily any computer network. This difficulty has come to be a common problem as well as is coming to be further hard to give rise to under supervision. The paper highlights various legal issues that are there due to cyber crime while analyzing the elements of the crime in reference to the cybercrime further the paper lays emphasis on how the cybercrime has affected the youth of the country and lastly the paper highlights various recommendations for the same.

INTRODUCTION

Cybercrime may be defined "as a voluntary and willful act or omission that adversely affects a person or property or a person's computer systems and made punishable under the Information Technology Act, 2000 or liable to penal consequences under the Indian Penal Code". Exact explanation of computer related crime is, it has not been statutorily explained in any act or law up till now. Even the IT Act, 2000 does not cover the explanation of cybercrime.

The foregoing definition of cybercrime clearly indicates that there exists very thin line of demarcation between conventional crime and cybercrime. The "sine qua non for cybercrime is that there should be an involvement at any stage, of the virtual cyber medium i.e., the computer and a simple yet sturdy definition of cybercrime would be, unlawful acts wherein the computer is either a tool or a target or both". Thus, cybercrimes are the crimes directed at a computer or a computer system or a computer network.[1]

FUNDAMENTAL ELEMENTS OF CRIME

To corroborate to anyone whether he/she is remorseful of any violation in criminal law, proof of actus reus and mens rea has to be proved excluding in stringent accountability violations[4]. Originally in Europe criminals were imposed many penalties, but they did not speculate mens rea as significant component. But after improvement in criminal law, afore assigning any penalty, they begin to evaluate mens rea as well as actus reus. Besides actus reus should be validated afar from a rational concern. There are two significant ingredients of crime viz.

ACTUS REUS IN CYBER CRIMES

Actus Reus defined as "such result of human conduct as the law seeks to prevent in cybercrime actus reus is highly varied and dynamic and in simple word actus reus means result of human conduct.it does not include mental element". It is not only limited to the regulation, but also includes state of affairs[2]. "C.J. Smith & B. Hogan found actus reus to be a product of human action because the law attempts to prevent it. Simply guilty intent is not adequate to resolve the criminal fault but any act or omission is required to complete the offence. In in cybercrimes".

[1] S.C. Sharma, "Study of Techno- Legal Aspects of Cyber Crime and Cyber Law Legislations", p. 86, (2nd ed. 2008).
[2] All you need to know about Actus Reus, available at https://blog.ipleaders.in last visited on January 31, 2022

Actus reus has[3] "become a challenge because the whole act was done in an intangible environment, the perpetrator may leave some mark on the computer and although it is a great challenge to testify in a court of law, as it is necessary to be in a physical condition or in a situation where they are allowed to testify. In cybercrime it is easy to find an actus reus but it is very difficult to prove".

Whenever an individual accesses a pc service, tries to acquire internet access, or transmits information via numerous PC, it might be regarded as an offence. The absence of permission on the side of prosecution is an essential element of "the actus reus in rape proceedings". If the prosecution has not been able to demonstrate such refusal of consent, the matter will be dismissed since the accused's actus reus doesn't really produce proof. Mens rea can be considered a portion of "the actus reus in" this situation.

MENS REA IN CYBERCRIME

According to current law crime can be committed with mens rea. Mens rea is a second major component of crime, sometimes called 'guilty guilt.' the definition of mens rea underwent a gradual change before modern criminal law was adopted as it often required a sense of guilt for a particular type or aspect of the mind.

Mens rea[4], refers to the individual's intention to perform an action. The action is still the same although the mood creates the action 'reus' so it has become a crime. Soon all the crime needs proof of some kind of mental size.

Many courts have concluded that 'especially every crime is in the mind' with each case requiring a clear attitude toward the rules in a particular section of the law: 'contempt', 'intentional', "malicious", "intentional", "unlawful", knowingly', 'fraudulent', 'by being unfaithful', 'by corruption', 'knowing or believing", "allowing" and "allowing" to express a wide range of different attitudes. However, the basic principles of a criminal case are motivation, negligence and knowledge.

[3] Farooq Ahmad, "Cyber Law in India- Law on Internet", p. 367, (2nd ed. 2008)
[4] Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both": In Indian Legal Perspective, available at https://www.mondaq.com last visited on January 4, 2022

Mens rea has been recognized as an integral part of crime without criminal charges where there is a strong obligation. Since the growth of cybercrimes, the legislative world has faced with the task of determining "mens rea in cybercrime", among other things.

If the prosecution has not been able to demonstrate such refusal of consent, the matter will be dismissed since the accused's "actus reus" doesn't really produce proof. Mens rea can be considered a portion of "the actus reus in" this situation.

There must be intention on the part of hacker to secure access, although that intention may be directed with any computer and not with a particular computer.

Therefore, the hackers do not need to be aware of exactly which PC he/ she was attacking. There are two important ingredients that make up the mens rea, in hacking, firstly access intended to be protected must've been unauthorized, and other as there should be knowledge on the part of hacker regarding the access[5].

IMPACT OF CYBER CRIME OVER YOUTH

Cybercrime will have a big effect on younger people. Today's teens form part of Gen Z, young people who were born and raised in the new technology era, who cannot envisage an offline world with no access to the Internet or social media. From an early age, they have juggled with computers, tablets and smartphones, accessories they use in their daily lives. In tandem, data also evidence that cybercrime is increasingly attracting and engaging with the teen population. Young adults are more likely than any other age demographic to access the Internet, because they are the first victims of cybercrime. This article would discuss how cybercrime impacts and creates challenges for younger generations.

Themes such as fitness, in particular emotional wellbeing, are addressed to explain the many cybercrime issues. Many younger people have been trying to kill themselves because they have been victims of cybercrime. This paper would examine all the consequences of cybercrime, including cyber bullying (a kind of cybercrime), and how young people may prevent cybercrime.

[5] Cyber Crimes And The Law In India, available at http://www.arjelaw.com last visited on December 23, 2021

TAGGING THROUGH PROFILES

Social networking sites like Facebook, Myspace and Twitter have taken social networking to new level. Users are often identified by their profile consisting of photos, basic information likes and dislikes, friends, school and family. Tagging is a feature which allows the user to label friends in a photo and link to their profile pages.

If tagged the user is notified so that the option is with the user to de-tag or stay linked with the comment, video or photo. The SNSs have features like location-based services which can be dangerous as it exposes the user's location and whereabouts.

The location-based service also has a feature that allows the user to tag where & who they are, at any given time. Children are unaware about the risk they are inviting by sharing with strangers the location with and of the family and friends.[6]

Tagging may serve as invasion of privacy, where the SNSs have 'tagging' option unless the user disables it, friends and strangers may be able to tag the user in post or photographs that carries personal information.[7]

Many SNSs like Facebook use the software to locate the location of the user, children and teens can also expose their location by tagging photos but if these apps are not used carefully, it can make children and teens vulnerable to exposing too much of their personal information like school, address, location, work or study.[8]

This feature also helps the online predators or the harasser to keep a track of the use of the child whom the predator intends to victim as he well knows that the original victim may not add or accept him in his friend list. The other way round the predator may try spying the victim by creating his own fake account to expose his identity as a child somewhat of the same age of the victim.

[6] Social Networking Safety, available at http://www.ncpc.org/topics/internet-safety/socialnetworking-safety last visited on January 24, 2022.
[7] Negative Impact of Social Networking Sites, available at- http://socialnetworking.lovetoknow.com last visited on January 29, 2022.
[8] NSPCC, available at http://www.nspcc.org.uk last visited on January 7, 2022.

CYBER BULLYING

Cyber bullying victims also face rumors and misinformation on social networks online. Bully pictures of their victims can seem indecent or shameful. The use of mean text messaging as harassment is another aspect of cyber bullying. The National Council on Crime Prevention says that over half of the American youth have problems with online bullying. The young took their own lives because of online bullying in some serious situations.[9]

CHILDREN AND CYBER BULLYING

Most of the following methods of harassment are classified as internet bullying when they have been carried out via electrical technology as well as appliances such as mobiles, pc, as well as tablets via chats, text messengers, or social media sites.

This dramatic rise in cyberbullying behavior that leads to child suicides cannot be ignored, as well as a system for prevention of the spread of these actions is urgently needed.

HARASSMENT VIA E-MAILS

This form of harassment is very popular by file attachments, sending letters, & links, i.e., through e-mails. Harassment is growing nowadays as the use of social media sites like Twitter, Facebook, Orkut, Instagram, etc. day by day increasing.

CYBER-STALKING

The phrase derives from the term 'stalking,' which means following a person to embarrass or harass that person.

If computer or email is used for commit stalking. It is often achieved by using certain criminal activities such as abuse of identity, extortion, defamation, spoofing etc.

Cyber stalkers[10] may create fake websites, create fake forums, send threatening spam, make fake profile or send harassing mails for stalk another person.

[9] Cyberbullying available at https://www.sciencedirect.com last visited on April 1, 2022.
[10] Jyoti Ratan, Cyber Laws & Information Technology, p. 48.

SEXUAL SOLICITATION

For teens who use cyber communications forms, sexual solicitation is increasingly concerned. It may occur on social networking platforms or in chat rooms. Sexual application takes place anytime an adult or a friend attempt to partake in sexual intercourse online. A teen could be required to share personal details, watch porn or talk about sex online.[11]About 70 per cent of teenagers online are females. Young people should be careful to put provocative images in chat rooms online and to speak with strangers.

TEENS ENGAGING IN CYBERCRIME ACTIVITIES

From the birth of the child, ethics and family rules play an important role in molding the child. Just as every family has its own rules and discipline every society has a system of rules usually enforced through a set on institution called Law. The object of which is to provide an objective[12] set of rules for governing conduct and maintaining order in society, thereby developing intimacy in relationships with peace and harmony.

One such instance involves videogame-related environments were coupled with tutorials offering tricks and tips for some videogames, they also show how to crack them or get hold of game licenses. "It is in these contexts that many adolescents are injected with the cyber fraud virus, to obtain products and services free of charge via hacking techniques, which may lead many of them to go even further and upscale their cybercrime activity".

And if people abide in the sense that the prefix cyber does not make the crime any less significant, severe or perilous for humankind, what they are discovering is teenagers who are initiating to reach into more consolidated connection with the crime. Whereas in the past, the criminal underworld could be specified and restricted from a structural and geographical end of stance, currently this doesn't subsist in cybercrime.

As it can be noticed from the current scenario of the world, is that even those who don't carry on to live or are brought up in the criminal world or in shoddy areas also see or endure a role in cybercrime.

[11] M. Dasgupta, Cyber Crime in India- A Comparative Study, p.8 (1st ed. 2009)
[12] Cyber Crime among the Youths available at https://www.legalserviceindia.com last visited on January 10, 2022.

This divulgence to criminality is furthermore transpiring at a more premature age, which is heading to affect these immature individuals' social values and faith learning approaches.

MOTIVATES SOME YOUNG PEOPLE TO BECOME CYBER CRIMINALS

Everyone[13] is aware that the cyber criminals are always searching for financial gain, but it looks that this is not generally what Young cyber criminals have in their mind when they take their first step over to the 'dark side'. The sense of achievement at completing a challenge, and justifying oneself to peers are the main motivation for those who involved in Cyber Criminalities.

Other important factor which draws numerous young people into the arena of internet crime is indeed the belief it's not a violation with in the further sense, or that people would not be jailed if they conduct an internet crime.

It underlines so for juvenile delinquents; money benefit is often not a primary focus. Rather, the satisfaction of accomplishing a task with the need to prove ourselves to friends in terms of improving one's personal brand seem to be the primary reasons for internet criminals. Dozens of lessons as well as online manuals exist which detail how to gain access to PC or steal information, or how to do all of these in surroundings, online networks, or internet site with adolescent stuff.

Several teenagers get infected also with internet crime virus in order to acquire incentives and rewards using hacking tools that might encourage many more to go forward as well as escalate their internet crime activities. And, if individuals remember that the suffix cyberspace doesn't really constitute the offense a little less severe, severe, or harmful for community, they will see that kids are becoming more involved in criminal activity.

CYBER CRIME SHOULD BE CONCERN FOR PARENTS OF TEENAGERS

Cyber Crimes is not an unease only for the Parents or Educators, also for Schools and Educational Institutions as a total. Every individual is an element of this simulated realm, as well as it is extremely hard to remain outside it.

[13] What motivates some young people to become cybercriminals? available at https://www.welivesecurity.com last visited on April 2, 2022.

Though, individuals possibly sense that computer-based crimes do not impact common circumstances on a lower position. With the unmanageable extent of public channels, cyber offenders have found fresh mass media to impulse forward the offense. Public channels like FB, Twitter, Insta, Snapchat, WhatsApp, as well as others comprehend the stress of computer-based crimes also hire a sullied computer-based misconducts finding device beside receiving valid assistance from the expert of the Social Law Network.[14]

1000 kids have been disclosed to the virtual realm at an initial age. They are shrewder in social media platform, common channel administration, appreciating application interface, as well as using technology for day-to-day difficulties. Uncountable teenagers adore attempting as well as investigating, as teenagers have always accomplished. Nowadays youngsters notify the young population to carry no anxiety about disclosing the complicated components of their existence on Twitter, FB as well as Insta.

They are probable to mark stupid or unpleasant opinions on other individual's webpages. Always they merge with wrong associations as well as mediums that are virtually available, conversations with outsiders, share their portraits as well as harm their private data by linking their personal information's on their mobiles, tabs, laptops, and other devices.

They are easily available as to be simple victims of computer-based offenders, they moreover place their homes as well as respected singles at threat.

PARENTS ROLE AND RESPONSIBILITY[15]

Social responsibility to protect children on internet is based on responsibly grounded ethics inculcated in the child from birth and set of rules that consider broad impact of family's responsibility towards children. Parents play a crucial role & are socially accountable (Article 51(A)) in the child's life, socializing and development.

Parents need to be the one trusted source children can turn to when things go wrong in their life, whether online or offline. Unfortunately, the primary as well secondary data collected in the empirical study during this research indicates that parents are the one source children avoid

[14] Importance Of cybersecurity In Education Sector In 2022 available at https://cybersecurityforme.com last visited on February 27, 2022.
[15] Shital Kharat, "Cyber Crime – A Threat to Persons, Property, Government and Societies", SSRN (2017)

when things go wrong online, as parents tend to overreact. Children avoid telling parents about cyber bullying fearing that parents will only make the situation worse.

The great challenge to the parents and guardians is to monitor and apply rules to something they have lesser knowledge of.

The few steps that parents and guardians may take to curb the menace of cyber victimization of children are as follows-

Get Involved Online

Try to learn, understand and use these tools and also the applications. The best way to approach a problem is to understand it fully and what better way than using the internet yourself to understand the potential concerns for your child. The more the parents are savvy of the computer and its online applications the better they will be able to tackle the risk factors associated with it. As a result, the parents would be well equipped to secure the safety and be able to protect their children online. Parents can then in turn educate their children about the internet technology and its privacy settings.

Online Method of Communication

Accept, understand and implement the method today's children are using to communicate, as they like to speak and communicate majorly with mobile phones and now with the added benefit of uploading photos and videos they use less of words. The best way is also constant and continuous communication with children about their online activity.

Parents should develop trust and teach their children online etiquette and behavior which will make them feel supported. As a result, the children will come to trust their parents as their lifeline if they encounter any online risk or offline risk for that matter.

Parents should be friendly[16] in communication and also warn about the online risk that their children might come across and how to deal with it.

If the child informs about any online risk encountered by him or her, the parent should be matured enough to handle this situation as it's their responsibility to guide the child to safety.

[16] Prabhash Dalei & Tannya Brahme, Cyber law in India: An analysis, 2013. IJHAS, volume 2, issue 1

Blogging, chatting and SNSs

Parents need to learn and experience the way in which blogging, chatting and SNSs work. This could be done by creating a user identity and visiting the websites which the child uses often.

Parents should set up their accounts and profiles on these SNSs not to spy but to supervise whether the children are safe online and educate them on the abuse they might encounter on these SNSs and how to prevent such abuse.

- **Place of Computer**

Place the computer in a room or area which parents visit often when children are online. Centrally locating the computer also enables children to immediately contact for anything that they feel uncomfortable with online[17].

Use another computer which will not have internet so that when parents are away from home and children need to work on a project or for a school assignment, they can make use of that computer.

- **Emergency Help Method**

If both parents are working and out of the house, they should set a system whereby children can contact them for any online danger that they may come across. This could be done via emailing, instant messaging and text messaging as a rapid way to alert the parents.

If the child encounters danger on line or has become a part of an online activity due to which a destructive situation has come-up in the child's life and the family, then the situation should be handled delicately, ensuring that the child is not blamed but made to understand the fault.

Moreover, the parent should find out ways to make them feel comfortable.

- Parents need to be aware about their child's basic rights, the internet, child abuse and cyber bullying and its many forms on the internet.

[17] Protection of Kids from Cybercrimes: Role of Technology Contracts available at https://blog.ipleaders.in last visited on January 26, 2022.

- Parents need to have knowledge of internet etiquette so that they inculcate them in their children and make them understand that the risks can be encountered due to unregulated use of the internet.

- Parents should restrict unsupervised internet of usage by children and guide them to visit only age-appropriate websites and also educate them so that they don't share any personal information and family details or photos online.

- Parents should use trusted and reputed Internet Service Providers. They should also ensure that they filter software on the child's laptop or personal computer at home and ensure that there is a firewall installed on it. Parents should discuss with children their pattern of internet usage.

- Parents should tell the children about predators and pedophiles and other potential risks the child may encounter. The children should be taught to report to the parents about any suspicious online activity.

- Parents should also request and insist the cyber cafes and educational institutes to have child protective measures including firewalls and filters.

- **Filtering Software:** Total reliance on costly filtering software is not effective as per the consumer reports magazine 2012. It says that internet filtering softwares[18] generally fail as one out of five objectionable sites slip through the filter and are not blocked.

IMPACT ON PRIVACY

Privacy includes the right to control any person's private details as well as the capability to decide in what way that information must be attained and utilized. "Right to Privacy is recognized as a fundamental right under Article 21 of the Constitution of India which deals with the right to life and liberty, although the right to privacy does not find an explicit mention in the Constitution, this has been recognized in various judicial pronouncements". Nevertheless, the consequences of the right to privacy in the computer-generated world aren't fixed problems. The probable privacy breach in social networking websites can be explained via instances of FB and Orkut.[19]

[18] Cyber-Crime, available at https://lexforti.com last visited on March 20, 2022
[19] Electronic Commerce available at https://www.techtarget.com last visited on February 4, 2022.

Orkut was once praised as one of the foremost famous SNS but lost its brilliance when Facebook arrived. Numerous people have not deactivated their accounts & thus they were open to the mass misuse of prudent confidential details. Search selection accessible on FB allows private data of operators to be visible to everyone who types the title in the search option.

Via choosing "Public in privacy settings with respect to information as gender, networks, username, email id, phone number, pictures and videos poses a risk to the identity of the person". Additionally, usage of applications as well as games available on virtual platform rush a serious peril toward individuality of the individual. Such programmed don't really operate together in safe manner. They also want accessibility to everyone's private details.[20]

Virtual attacks on networking sites are commonly regarded like a violation for data protection rules. A person's information like title, residential information, passion, blood relations as well as so on are frequently accessible on numerous networking sites. In our country, protection of information is overseen by Sections 43A, 72A, 69 as well as 69B of the Information Technology Act.

Sec. 43A broadens the range of "data protection by inclusion of definition of Sensitive Personal Data or Information", as well as levies an obligation for "Reasonable Security Practice to be followed by the data handlers and in case of infringement, data handlers and cyber offenders can be slapped with an exorbitant penalty which may even exceed Rs. 5 crores".

"Section 72A specifies liability for intermediary if he discloses personal information which he accessed while providing services under a contract and such disclosure was made with an intention to cause or knowledge that he is likely to cause wrongful loss or wrongful gain to a person". Sections 69 and 69B authorize the government to give instructions intended for capture, observing as well as gathering of circulation data or info. over any computer source for cyber safety.

LEGAL REFORM

Intensification of regulative incorporation of the UNCRC 1989 on 26th day of November 1949 the Constituent Assembly of India adopted, enacted and given to ourselves the Constitution

[20] Electronic Signature: Legal and Technical aspect available at http://www.legalservicesindia.com last visited on January 19, 2022
[30] Laws Against Hacking In India available at https://blog.ipleaders.in last visited on January 7, 2022

which shall come into force on 26th January 1950. At that point of time UNCRC 1989 was not in force and as India is a signatory to UNCRC and had adopted it to frame its laws and regulations in consonance with international regulations. Article 51 of the Constitution envisages that "The State shall endeavor to promote international peace and security; maintain just and honorable relations between nations; foster respect for international law and treaty obligations in the dealings of organized peoples".

In this context, certain legislative changes if needed he are to be made in the basic law of the country and also other legislation. Part III & Part IV of the Constitution of India include provisions for survival, development and protection of children, pertaining to 'Fundamental Rights' and 'Directive Principles of State Policy.'

With the ratification of the UNCRC and article 15 (c) of the Constitution of India it becomes the prime responsibility of the Government of India to effectuate the obligation undertaken through ratifying various international treaties and global policies to address the child issue.

The Government of India has accepted and ratified the Convention on the Rights of the Child, whereby an administration of customary laws was undertaken to boost the new landmark legislation - Protection of Children from Sexual Offences Act, 2012 (POCSO), in assimilating the basic standards embraced in the UNCRC 1989, wherein all appropriate national, bilateral and multilateral measure to prevent child from exploitation and sexual activities is addressed.

This act has special focus on the sexual exploitation and assaults on children. Though this act is special act addressing child pornography but a few changes with insertion of provisions addressing the topic of my research will be more beneficial to the society. "The IT Act[21], Juvenile Justice Act, IPC, and Young Persons (Harmful Publications) Act, 1956, must be adopted in the scope 'invasion of privacy' without interference of the adult world in the innocent lives and to live a dignified life as established in Article 21 of the Indian Constitution and directive 39 (f) and Article 16 of the UNCRC".

In order to reside a decent as well as self-respecting lifestyle inside the internetcommunity, priority must be paid to basic issues such as bullying, online harassment, misuse of personal information, as well as reputational loss. As a result, further significant difficulties arise, like aiding in euthanasia as well as along-term impact just on brighter welfare. Kids have been

[21] The Information Technology Act, 2000 (Act 21 of 2000

attacked here on net, particularly on online communities, due to an absence of meaningful internet regulations as well as social consciousness just at local level within different components of community, as well as a proper analysis of cultural components.

MODIFICATION OF THE PRESENT POLICY FRAMEWORK

Our country is no longer a participant to the EU Conventions on internet crimes as well as therefore does not participate in the summit. Our country has no cybercrime program or internet programmed. Currently the world-wide internet crime agreement with our country are two diverse aspects. "A new set of synchronized legal frameworks to fight cybercrimes through international cooperation will prove to be accommodating in combating cyber bullying in India".[22]

Strict internet law as well as strategy structure solely for shielding youngsters online is the pressing priority. As there are no guidelines to deal with virtual crimes on web and the crime like cyberbullying goes unseen and undiscovered on social media sites. The Protection of Children from Sexual Offences Act, 2012 (POCSO) which was enacted as outcome of a survey in 2007 stating that- forty percent of children in India are below 18 years of age and fifty three percent children surveyed in 2007 had experienced one or other forms of sexual abuse.

The same reasons are in the current Indian scenario where India stands third on the globe in cyber bullying with fifty three percent of Indian children between 8 to 17 years been bullied online there is an urgent need for laws to protect children from online bullying. Separate provisions can be inserted in the POCSO for preventing cyber bullying, online harassment of children, online defamation and invasion of privacy in cyber space.[23]

The appreciable part of the Act is its flexibility that reflects in its section 45 that allows the Union Government to make the necessary changes in the Act whenever and wherever need arises as per the situation and the power to make rules rests with the Central Government. As such section I POCSO- the Act may change its principal tittle by removing the term protection and replacing it by 'prevention and prohibition' the word 'harassment' may be introduced after the word 'offences' such that the revised tittle should read 'The Sexual Offences and Harassment of Children (Prevention and Prohibition) Act, 2012.

[22] Technological developments and the future of cybercrime available at https://www.rand.org last visited on January 4, 2022.
[23] Cyber safety for school available at https://megcentre.kvs.ac.in last visited on February 5, 2022.

The insertion of the term harassment then can be bought with several subsections within its scope which can cover, invasion to privacy on internet, defamation, harassment, and consequences of entering into a contract, abetting to suicide.

Section 2 – This section may insert the definitions of terms harassment, bullying, intimidation, abetment to suicide and various offences, victim and accused in accordance with the IPC, Juvenile Justice Act, and formation of contract as per the Indian Contract Act. The definition of "cyber bullying can be similar to that of section 354D[24] of the Criminal Law (Amendment) Act 2013 with a slight change by replacing the term women by- women and children". The imprisonment should be not less than five years and a hefty fine should be imposed.

Under Chapter II, below clause E there may be a new clause F with sub-section 12(a) which may define harassment and course of conduct, 12(b) There may be civil remedies sought by the way of compensation directing the accused to pay the victim. 12(c) may impose the punitive provisions for the new offences defined in the above sections. These Prohibitory punishments must be made in accordance with the IPC sections that attract the concerned crime and also section 66A of the IT Act.

Under Chapter IV, there may be inserted sub-section in section 16 as 16(a) abetment to suicide – Which may extend the harassment and bullying caused to an extent to drive the victim to suicide by the way of mean annoying messages, causing fear in the mind of the child and making him or her feel ashamed and insulted, thereby harming the reputation, which may cause to abetment of suicide 16(b) may have civil remedies of compensation, but should necessarily have prohibitory punitive measures in accordance of section 305[25](abetment of suicide of child or insane person) and 306[26] (abetment to suicide) of IPC.

The Chapter V which reads as "Procedure for Reporting of Cases" under section 19 a new clause addressing the failure on the part of the police officer of the concerned police station to register the complaint when approached by the victim or his or her parents may be inserted. Such refusal or negligence of the police officer to take immediate action on a complaint may be counted as offence committed by the officer in course of his duty. And the cognizance can be taken in accordance with section 78[27] of IT Act.

[24] The Criminal Law (Amendment) Act (13 of 2013), s. 354 D
[25] The Indian Penal Code, 1860 (Act 45 of 1860).
[26] The Indian Penal Code, 1860 (Act 45 of 1860).
[27] The Information Technology Act, 2000 (Act 21 of 2000), s. 78.

The other procedures may be in accordance with the Juvenile Justice Act and the POCSO which mandates the law enforcement to have the presence of a lady police officer right from the beginning. With so many cases of cyberbullying ending with child suicide there may be a clause in place that will authorize the immediate reporting and investigation of cyberbullying cases where the investigating officer may have a precautionary measure against SNS and ISPs whether situated in or outside our country. Non-compliance with instant act regarding complainant's appeal as well as contract fissure.

Since SNSs are within their policy of deleting content when reported by the victim or parents but often ignore that request, there should be a law in place to prosecute them for nonfulfillment with their draft procedure guiding principle.

RECOMMENDATIONS

- On government's part, measures shall be taken to implement regulations of existing preventive laws, Government shall also ensure broadcastingto masses about ensuring safe and sound behavior in cyberspace.
- The education of computers at school level is mostly technical in nature.This has to expand beyond the limits of learning basis and making students aware of cybercrimes and how they could prevent it effectively.The education shall also cover other important aspects like bullying prevention and secured internet surfing.
- Holding public meetings for promoting positive utilization of the internet. Such meetings shall also cover other simple yet effectivepreventive steps that could be taken at individual level, like changing ofpasswords frequently, not sharing of personal information with strangersand keeping community update about recent advancements and about taking requisite security steps against cybercrime victimization.
- Cyber policing needs to be all time active, Indian police may collaboratewith police of other advanced countries and sharing of knowledge wouldhelp police be better prepared for dealing with intricacies associated with cybercrime investigation.