MULTIDIMENSIONAL CYBER THREATS AGAINST CHILDREN

Dr. Shipra Gupta[1]
Associate Professor,
Department of Law,MMDU
Mullana, Ambala

Ms. Madhu Sangroya[2]
LL.M. (Student)
Department: Law, Rayat Bahra University,
Mohali, Punjab

ABSTRACT: Today the most common threat isn't the man who owns a missile; but a man 2000 miles away who has the password to fire it. Since the beginning of civilization man has always been motivated by the need to better the existing technologies. Today, keyboard has replaced the gun and is a more powerful tool. Development of internet fostered the crime to acquire cyber dimension leading to the huge problem of cybercrime by potential criminals in cyberspace. Child abuse is finding new forms and channels through mobile and digital technologies. Children, since inception have been victimized due to lack of education, social stigmas and potential threat of social harassment making them soft targets of cyber criminals. This paper would give an analysis that how effective or ineffective the laws are in combating this crime and will delve into experiences of people shedding light on the various forms of social media crimes.

1. INTRODUCTION

The exemplary growth of social media in the last decade has redefined the communication systems and framework via internet amongst individuals. Social media refers to the collection of all the communication channels and networks by way of which information flows, interactively received and disseminated at receiving end. Popularity and wide acceptability of social networking sites such as Facebook, Twitter, LinkedIn, and Google plus as a medium of instantaneous online as well offline data sharing portals serves as a perfect example of growth and prominence of social media as a means of communication in our daily life. According to Neilsen, a contemporary internet user tends to devote proportionally more time on social media sites rather than on any other type of site. This leads to sharing of minute to minute professional and personal content in open source which can be accessed and exploited by anyone at the same time. This acts as a gold reserve for the cyber offenders to exploit the data of the victim to generate wrongful gain in his favor by causing wrongful loss.

Therefore, social media crimes refer to all forms of crimes which tend to exploit social media networks and platform for commission of certain offensive act. According to John Cooper QC, "the vast majority of people who use the social media are like society. The vast majority are decent, intelligent, inspiring people. The problem comes with a small minority, as in society, who spoil it for everyone else.[1]According to the Guardian, crimes linked to the use of Facebook and Twitter have increased by 780% in four years, resulting in about 650 people being charged last year.[2] Today the act of 'newspaper reading or watching television' got replaced by acts of posting, tweeting and 'going viral'. Professor Michael Whalen says that one British study found that a high percentage of the burglars they interviewed admitted to using social media sites when

---

[1] Social Media and the Law, Parliament of UK, available at: http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3704.htm

[2] Social media-related crime reports up 780% in four years, The Guardian, Dec 27, 2012, available at:http://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter

choosing their targets[3]. For example a person's Facebook update displaying that he will be out in the night gives the burglars a quality time to bust into the house and property. The social media portals like Facebook,Twitter, LinkedIn which promotes users to post profiles of themselves further narrowing it touploading pictures, interests, and events attended helps as a trap setters and a source which is exploited by social media criminals to commit crime as today gathering open source information can easily compromise a person'sprofile by catching him in a honey trap. Apart from it these social media criminals take benefit of their ambiguity, anonymity, confidentiality, and interconnectedness provided by the Internet. For example Google Street View is misused to gauge the victims' properties over the Internet. Some of the well recognized social media crimes affecting netizens range from-

- Cyber bullying,
- Cyber stalking
- Defamation (Fake profiling, Abusive posts, obscenity)
- Cyber trafficking and pornography
- Morphing
- Sexting (texting via using offensive sexual terminologies, procurement of nude pictures and suggestive material)
- Child pornography (virtual prostitution, Honey traps)

CHILDREN: PRIME TARGET OF CYBER CRIME

Gender manifested crimes and subsequent subjugation of children as sex object around the globe has sprouted up cutting across borders and culture. Since the exponential growth of electronic, computer based communication and information sharing via internet there has been emergence various internet based medium facilitating major forms of child maltreatment, sexual and emotional abuse. Despite this, only five per cent of children across the world had access to the Internet in 1999 (UNESCO (United Nations Educational, Scientific and Cultural Organization) 2001). In the United States, the nation with the highest usage, 63 per cent of 501 surveyed 9-17 year-olds, stated that using the Internet was a preferred pastime over watching television. Research in the United Kingdom has found that "the greater the chance to use computers that children get, the greater their desire to use them more".

The anonymity and false identities of the offenders facilitates the sexual exploitation and exchange of inappropriate material with children who easily secure private access to internet. Anonymity acts as a tool in deceiving children to be a trusted friend or a caring parent figure. An offender may lurk in Internet chat rooms, gathering information until an opportunity arises to move the conversation with a child to a private chat room or to a mobile phone, and then ultimately arrange a real life meeting

The children who are emotionally immature, who have experienced prior mal treatment and children with learning disability, problems with peer friendship or deprived of love and attention become easy targets of online abusers. A study of children aged 10-17 years in the United States found that children over 14 years who were "troubled" were more likely to be solicited.

According to the Global statistics, 85% of parents up to age of 13-17 years report that their child is on social networking sites.[4] About 29% of Internet sex crime relationships of the teenagers were initiated on social media sites.[5] This was further elaborated with case studies indicating that in 26% online sex crime against minor

---

[3] Crime and Social Media Sites – Catching Criminals and learning to avoid them, Jared Newnam, available at: http://source.southuniversity.edu/crime-and-social-media-sites-catching-criminals-and-learning-to-avoid-them-75131.aspx

[4] American osteopathic Association, 2011

[5] Journal of Adolescent health 27, 2010

women offenders disseminated pictures and information through victims' social networking site.[6]As many as 80,000 cyber-crime related complaints have been registered with police in Kerala in 2012, of which 50,000 relate to harassment of girls through new hi-tech devices.[7]

FACTORS MAKING CHILDREN VULNERABLE TO THESE CRIMES:

- **EDUCATIONAL BACKWARDNESS**

Due to lack of adequate knowledge and awareness children fail to understand the vices of the social media and are prone to getting trapped as baits of social media offenders. Failure on the part of the user regarding awareness about the minimum age to join cyber communities and portals like facebook, Twitter, Instagram with subsequent illiteracy about password sharing, states the lack of cyber hygiene amongst citizens today.

- **LEGAL BACKWARDNESS**

The Information Technology Act, 2000 inherently covers the commerce related crimes. Cyber defamation, email spoofing, cybersex, hacking and trespassing into one's privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions[8]. Therefore IPC along with the 2013 Criminal Law Amendment Ordinance, further supported by the Prevention of children from sexual offences try to fill in the lacunas existing in the cyber legal framework for users or netizens.

- **SOCIOLOGICAL BACKWARDNESS**

"Culture is the sphere where we socialize ourselves, and the Internet – global in its reach – is a dimension of that sphere." Jeremy Rifkin

Children since ancient time have been kept under the persistent surveillance of their guardians and have to observe strict norms of social conduct with subsequent regulation from orthodox customs. This has hampered the growth of children especially girls and thus reduced them to mere carriers of family's pride and status symbol. Today this has lead to inexpedient circumstances wherein these societal hindrances under the umbrella terms of defamation to family reputation, shyness and hesitancy have lead to failure in reporting and registering of the cases of cyber violence against children. Therefore, acquainting citizens with technology is productive facet that can be accepted fundamental for the advancement and evolution of any country.

CHILD PORNOGRAPHY

The word "porne" stands for prostitute and "graphein" stands for documentary. It can even refer to portraying of sexual content on the internet portals. Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. It has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive[9]. Majority of developed countries do not object to adult pornography but have stringent laws for child pornography all across the globe.[10]

---

6 Ibid.

7 The Indian Express (2012) "Cyber bullying new-age threat" Indian Express, Nov 24 available on: http://newindianexpress.com/cities/bangalore/article1352590.ece

8 Abhimanyu Behera, " Cyber Crimes and Law In India," XXXI, IJCC 19 (2010)

9 Cyber Pornography and the IT Act, Asian School of Cyber Laws, available at: http://www.police.mizoram.gov.in/uploads/files/cyber-pornography-it-act.pdf

10 Online Pornography, available at: http://gurgaon.haryanapolice.gov.in/online-pornography.htm

According to Gillespie: *"Interpol defined child pornography as ''any means of depicting or promoting the sexual exploitation of a child, including written or audio material, which focus on the child's sexual behaviour or genitals''*

Legal provisions pertaining to child pornography:
Section 67B (20) of the Information Technology Act, 2000 states the punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

In the case of ***Janhit Manch & Ors. v. The Union of India***,[11] the petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

The Protection of Child from Sexual Offences Act, 2012 also provides for punishment regarding child pornography. Chapter 3 of the Act is titled Using Child for Pornographic Purposes and Punishment in which Section 13 to 15 provides for punishment for using a child for pornographic purposes and punishment for storage of pornographic material involving a child.

In ***Court on its own motion v. State of Punjab,*** it was held, "We would like to mention that recently, the Parliament has enacted the 'Protection of Children from Sexual Offences Act, 2012'. This is an Act to protect children from offences of sexual assault, sexual harassment and pornography. It becomes necessary to have effective implementation of this enactment as well. Under the Act, the National Commission and State Commissions have been made the designated authorities to monitor the implementation. Rules, 2012 have also been framed under this Act and Rule-6 prescribes for such monitoring with specific functions assigned to National Commission and State Commissions. Needless to mention, National Commission as well as State Commissions shall start discharging their functions under this Act in a meaningful manner."

In ***Avinash Bajaj v. State (N.C.T. of Delhi),***[12] "the law in our country is not adequate to meet the challenge of regulating the use of the internet to prevent dissemination of pornographic material. It may be useful to look at the legislative response in other common law jurisdictions. In the United States, there have been three legislations that have dealt with censorship of pornographic material on the internet: the Communications Decency Act (CDA), which was enacted as a part of the Telecommunications Act, 1996, the Child Online Protection Act, 1998 (COPA) and the Children Internet Protection Act, 2003 (CIPA). The CDA sought to prohibit the use of an interactive computer service to send or display in any manner to those under the age of 18, any communication that depicts or displays sexual or excretory activities in a manner that is patently offensive.
In ***Kamlesh Vaswani v. Union of India***,[13] it was held that the websites showing child pornography, especially of children between 14 to 18 years should be strictly banned. The court stressed upon the seriousness, importance and urgency of the matter and directed that, all parties by the said order must take positive steps to try and contain the menace of child pornography. Further directions issued to the Secretary, DoT to file personal affidavit within one week on issue as to whether DOT or any other department of Government of India is competent to issue direction to call off sites showing pornography.

CYBER BULLYING
Bullying means systematically and chronically inflicting physical hurt or psychological distress on one or more students. It is further defined as unwanted and repeated written, verbal, or physical behaviour, including any threatening, insulting, or dehumanizing gesture, by a student or adult, that is severe or pervasive enough to

---

[11] 10.03.2010 Public Interest Litigation

[12] (2005) 1 CCR 265

[13] (2014) 6 SCC 705

create an intimidating, hostile, or offensive educational environment; cause discomfort or humiliation; or unreasonably interfere with the individual's school performance or participation; and may involve but is not limited to: teasing, social exclusion, threat, intimidation, stalking, physical violence, theft, sexual, religious, or racial harassment, public humiliation, or destruction of property.[14]

Cyber bullying takes different forms: threats and intimidation; harassment or "cyber-stalking" (e.g. repeatedly sending unwanted texts or instant messages); vilification/ defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images (including what are sometimes misleadingly referred to as 'happy slapping' images); and manipulation performed on social media, such as Facebook, Instagram, Snapchat, and Twitter, SMS (Short Message Service).Research carried out for the Anti-Bullying Alliance (ABA) by Goldsmiths, for example, found that 22% of 11-16 year-olds had been a victim of cyber bullying.[15]It leads to depression, higher level of anxiety, somatic complaints and suicidal ideations. Whereas in long run it leads to externalizing problems such as increased delinquency and substance abuse than their no bullied peers.[16]

LEGAL PROVISIONS PERTAINING TO CYBER BULLYING

Chapter 11 of the Information Technology (Amendment) Act consists of offenses, where there is no clear definition of the offence of cyber bullying. Still the Act provides remedies againstthe same under section 66 and section 67.

Modes of bullying can be through e-mails, threatening, or even posting false statement which causes injury to the victim not only physically but psychologically. Section 66A provides remedies against offences which involve sending of offensive messages through a communication service. It gives punishment for an act which involves sending of information which is offensive, or false, or points out the character. It also deals with punishing the minds whose purpose is to cause danger, insult, injury, enmity, danger, hatred, ill will etc. to the victim, through a computer resource or by communication devices.

Bullying using someone's account without the consent or knowledge of the owner is also common. This results in action against the owner. The remedy available to the owner against the bully is provided in the section 66C. Section 66C punishes a person who commits theft of identity, that is, if any person uses other person's unique identification element, password or even digital signature which is unique. The punishment extends up to three years and also fine up to one lakh.

Posting nude pictures is the worst kind of bullying which has severe effect on the victim. Such bullying can be punished under section 66E. Section 66E punishes an act of the bully where the accused violates the privacy of the victim by posting, sending, printing photos of victim's private area, without the consent. Even capturing such photos intentionally is punishable. The punishment is a term of imprisonment which may extend up to three years or with fine up to two lakh rupees, or in some cases, with both.

CASE STUDIES OF CERTAIN SECTIONS UNDER THE INFORMATION TECHNOLOGY ACT, 2000

Section 66A – Punishment for sending offensive messages through communication service

Fake profile of President posted by imposter

---

[14] "Anti-bullying laws in India" Bar Association of India, 2015, < https://www.indianbarassociation.org/wp-content/uploads/2015/11/Anti-bullying-laws-in-India.pdf

[15] P. Smith, J. Mahdavi et al 2006

[16] Current perspectives: the impact of cyberbullying on adolescent health.*Nixon CLAdolesc Health Med Ther. 2014; 5():143-58.*

On September 9, 2010, fake profiles of the Hon'ble President Pratibha Devi Patil were made on social networking website, Facebook. The First Information Report Under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the Economic Offence wing.

Section 66E – Punishment for violation of privacy

Jawaharlal Nehru University MMS scandal

Two students of the renowned and prestigious institute – Jawaharlal Nehru University, made a pornographic MMS clip of a girl in the campus and circulated it outside the university. Initially they tried to extort money from the girl in the said clip but after failing, the culprits circulated the video out on mobile phones, on the internet and even sold the clip as a CD in the blue film market.

Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Janhit Manch & Ors. v. The Union of India, 10.03.2010 Public Interest Litigation[17]

The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

SAFE SURFING MEASURES

It only takes a little bit of effort, a few tools, and some basic information to be safe as you browse the Internet.[18]

- Update Web browsers regularly and enable security features.
- Install protective software
- Use Parental Control Software. Stay in loop.
- Place the computer in highly trafficked area.
- Set limits on night use.
- Guard personal information
  Look for signs of an encrypted Web page when providing sensitive personal information (credit card or banking information, SSNs, etc.) online.
- Read the privacy policy of the applications thoroughly –
  For example, the new feature of Whatsapp enables and promises on one front end to end encryption but at the backend it clearly specifies in the policy that it has the power and autonomy to go through the data and stop its publication under certain circumstances.
- Type the address of your social networking site directly into your browser
- Choose your social network carefully.[19]

---

17 PIL NO.155 of 2009

18 Northwestern university website, http://www.it.northwestern.edu/security/browsing.html

19 Ibid.

CONCLUSION

The research paper mainly focuses on the new age cyber threats faced by children. The IT Act, 2000 has failed to evolve and incorporate changes which have become imperative with time. Hence, the amendments of 2008 are not holistic and more changes are needed to make it more tropical with the need of the hour. A constructive approach securing the vulnerable, primarily children should be adopted while amendment. The growth of social media and the betterment of the existing technologies have led to the world becoming virtual. As the world has become cyber, so have the crimes. This paper has shown children being the major target of cybercrime due to the backwardness experienced by them.

Clearly, increasing online security is not simply a matter of not sharing passwords, contact details or photographs to strangers. Nor is it creating more stringent legislation that forces internet service providers to disclose customers' information and mandates that internet cafes register and take photo identification for all customers. While legislation is certainly required to ensure the realization of communication rights for both internet users and non-users, the dangers of increased policing of the web in both physical and virtual spaces and its impact on marginalized groups must be clearly examined. Lack of cooperation and support from foreign-based websites is just one of many hindrances to the resolution and eviction of cybercrime cases. Other factors include understaffed cybercrime cells within police departments; lack of IT knowledge of police officials, judges and prosecutors who must then rely on private professionals for expert help who are very few in number; and legislation that does not provide existing cybercrime cells with enough authority to take cases to completion. Hence,it has become imperative to strengthen the security mechanism which has been neglected for a while to ensure a secure cyber world for children.