DOI: *https://doij.org/10.10000/IJLMH.115293*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 3

2023

Cyber Law in Relation with Children

Manoj Kumar[1]

Abstract

This abstract examines the challenges and implications of children in conflict with cyber law. With the proliferation of technology and internet access, children are increasingly exposed to online platforms and digital communication channels. However, this expanded digital landscape also exposes them to potential risks and legal dilemmas. This abstract aims to shed light on the complexities faced by children in cyberspace and the importance of balancing their protection and accountability.

The prevalence of children's online activities and the rise in cyber-related offenses involving minors are discussed. Cyber law encompasses various areas such as online harassment, cyberbullying, identity theft, privacy invasion, and unauthorized access to computer systems. Understanding the intricate balance between protecting children's rights and ensuring their accountability is crucial.

Children in cyberspace face unique vulnerabilities due to limited digital literacy, lack of awareness regarding legal consequences, and susceptibility to online manipulation and exploitation. Parents, educators, and policymakers play vital roles in providing guidance, education, and safeguards to empower children to navigate the online world responsibly.

The abstract explores legal frameworks and initiatives designed to address children's involvement in cyber law violations. International conventions, national legislation, and regulatory efforts aim to protect children's rights online, foster digital citizenship, and enforce effective mechanisms. Cross-border jurisdiction and international cooperation are key challenges in effectively addressing cyber-related offenses involving minors.

Long-term impacts of children's encounters with cyber law are discussed. Restorative justice approaches focusing on rehabilitation, education, and promoting positive online behavior are highlighted. Creating a supportive environment that enables children to learn from their mistakes and become responsible digital citizens is essential.

In conclusion, this abstract raises awareness about the multifaceted issues surrounding children in conflict with cyber law. Comprehensive strategies encompassing legal, educational, and societal dimensions are necessary to safeguard children's well-being, rights, and future in the digital age.

Keywords: *children, cyber law, online activities, vulnerabilities, legal frameworks, digital citizenship, restorative justice, digital literacy, cybercrime, bullying, spamming, pornography.*

[1] Author is a Research Scholar at Radha Govind University, Ramgarh, Jharkhand, India.

I. INTRODUCTION

"Any technology tends to create a new human environment " - Marshall McLuhan

Marshall McLuhan declared above quote over forty years ago. Indeed, today's technology has created many new human environments and behaviours. The technological changes are boon for mankind and the Internet has changed the life of people altogether. One can communicate across through e-mail. The data can be downloaded or sent anywhere in n social networking sites have facilitated contacts with near and dear ones are being conducted online. Almost everyone is accustomed to the virtual and accesses the same. However just like the real world the virtual world from crimes. The persons committing the crimes are technological savvy of crimes that can be committed are social crimes e.g. cyber stalking; financial like credit card frauds, intellectual property crimes; crimes against state terrorism etc.. The crimes may specifically target the computer system or t may be used as a medium to commit crimes. In such a situation it was to leave the cyberspace in uncontrolled situation. This had led to passing Information Technology Act, 2000. The Act, initially covered fewer cyber crime but was amended in 2008 to include some more crimes. The POCSO is a significant piece of legislation that governs the protection of children from sexual harassment. The Act's provisions prohibit sexual assault, harassment, and pornographic material. The usage of computer technology and the Internet for teaching and education will rise if the current trend holds. Research into computer and Internet deviance is urgently needed. The goal of this study was to learn more about how middle and high school students perceive inappropriate online behaviours. For the past ten years, the Internet and computers have radically changed the way schools interrelate with the world. The information super highway has become a reality. Children can use the Internet from home or school to travel vicariously all over the world, to gather information and new knowledge. As more travel on this electronic highway increases, maps to find information and rules to keep the journey safe is becoming vital to successfully completing the journey. The Internet is the electronic highway that provides a means of instantly accessing people, institutions, and an overwhelming amount of information from around the world. Basically, the Internet is the world's largest computer network linking millions of people in world web, on every continent of the globe. Most of the services are provided free by organizations that support host computers on the network. These typically include universities, corporations, governments, and small businesses that use mainframes and mini- computers to maintain and manipulate databases. Children face a number of academic and behavioural challenges within the educational environment, including bullying involvement Due to the easy access of information on the Internet; the opportunity for misuse increases. Ethical behaviours by students, teachers, have become a major topic of concern. With the frequency of technology use, cyber attacks are also on the rise.

II. CYBER LAW IN INDIA

Cyber law is a term used to describe the legal issues related to use of communication technology, particularly “cyberspace”, i.e. The internet. it Is less of a district filled of law in the way that property, privacy, freedom of expression and jurisdiction, in absence ,cyber law is an attempt to applies laws designed for the physical world, to human activity on the internet. The information technology act of 2000 known as cyber in India.

In modern society right to privacy has been recognized both in eyes of law and in common parlance. Article 21 protects the right to privacy and promotes the dignity of the individual. Concern over the vast amount of personal data saved in computer files has grown over the past few years. The term "right to privacy" refers to the particular ability of an individual to control the collection, use, and dissemination of personal information. A few examples of personal information include hobbies, routines, and activities; family and educational records; communications (such as mail and telephone records); and financial and medical records. An individual could easily be harmed by the existence of computerised data about him/her which is inaccurate or misleading and which could be transferred to an unauthorised third party at high speed and at very little cost. Although the usage of personal data is increasing, there are many advantages as well as potential drawbacks. The fusion of technology has also given rise to new concerns around data protection and privacy rights. Innovative technologies facilitate communication and access to personal data. Data protection and the right to privacy are inherently at odds. Data protection should primarily reconcile these conflicting interests to information. But, the data of individuals and organizations should be protected in such a manner that their privacy rights are not compromised.

The Information Technology Act which came into force in the year 2000 is the only Act to date which covers the key issues of data protection, albeit not every matter. In fact, the Information Technology (Amendment) Act, 2008 enacted by the Indian Parliament is the first legislation, which contains provisions on data protection. According to section 2(1) (o) of the Act, "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed or is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer". The IT Act doesn't provide for any definition of personal data and, the definition of "data" would be more relevant in the field of cyber-crime.

III. Cyber crime

Information technology offences have been taken to encompass any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer system.[2] Cyber crimes have been on a rise at rate.[3] Undoubtedly, the criminal class has taken up the new at a much greater speed than our lawmakers and law e agencies. It has startled the world as much as the Inter amazed them. In 1888, an inspector was quoted in the Chicago Heralad affirming "a well-known fact that no other section of the avail themselves more readily and speedily of the latest science than the criminal class".[4] Can there be a greater t the Internet is concerned? In order to understand how people commit computer crimes, it is important to understand first why they do so. Obviously, the motivation for computer related offences is as varied as the motivation for any other type of crime, and may run the gamut from personal enrichment, avarice, revenge, and thrill seeking, to truly psychopathic behaviour. In general, virtually any type of offence, which can be committed without a computer, can be committed with the assistance of computers, including terrorism, espionage and obscenity. However, there are a few characteristics, which make computer crimes unique among criminal offences. For example, computer crimes may be committed remotely and across geographic boundaries. They may have effect years or decades after they are launched or planned. They may or may not violate 'traditional' criminal laws like trespass or theft statutes. They are difficult or impossible to investigate, and even more difficult to prosecute. Investigators, prosecutors, judges, lawyers and juries are frequently unfamiliar with the technology and its application, further complicating the prosecution of such offences.[5] Also, important for our analysis, as pointed out.

(A) Types of cyber crime

a. Cyber Bullying

Based on the social-ecological framework for bullying, which is an adaptation of

[2] Council of Europe: Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology, adopted by the Committee by Ministers on 11 September 1995.

[3] In a survey by the CSI (March 12, 2001), 85% of respondents, primarily large corporations and government agencies, detected computer security breaches within the last 12 months. 64% acknowledged financial losses due to computer breaches. 35% were willing and/or able to quantify their financial losses, which amounted to $377,828,700 in financial losses, up from $265,589,940 in 2000. The most serious financial losses occurred through theft of proprietary information. See, http://www.belmontpress.com/statistics.htm.

[4] Carolyn Marvin, When Old Technologies Were New . 1988.

[5] Mark D. Rasch, "Criminal Law and the Internet", at http://www.cla/org/ RuhBook/chpl l.htm.

Bronfenbrenner's (1977) Social Ecological Model of Child Development, individual factors are influenced by exposure to complex social and environmental factors, including family, peer, school, community, and societal interactions imbalance, and repetition and reinforced through group dynamics. Unfortunately, bullying has been linked to a number of detrimental psychosocial outcomes. Scholars have attempted to establish predictive profiles for youth involved in bullying. These profiles include bully perpetrators, where it has been argued that self-esteem is predictive of bullying behaviours. Children and youth who are involved in cyberbullying are also quite likely to be involved in "traditional" forms of bullying. In a study of middle school students, 61% of cyber "victims" also reported being victims of "traditional" bullying; 55% of cyber "bullies" also said they had bullied others in "traditional ways." Cyber "bully/victims" (who cyberbully others and also are cyberbullied) were heavily involved in "traditional" forms of bullying—64% had been bullied and 66% had bullied others.[6]

Cyber bullying can involve:

- Sending mean, vulgar, or threatening messages or images.
- Posting sensitive, private information and/or lies about another person.
- Pretending to be someone else in order to make that person look bad..
- Intentionally excluding someone from an online group.
- Children can cyber bully each other through:
- Emails
- Instant messaging
- Text or digital imaging messages sent on cell phones
- Social networking sites
- Web pages
- Blogs
- Chat rooms or discussion groups
- Other cyber technologies

b. Cyber theft

It refers to unauthorized acquiring of any information available on a computer system by

[6] (Kowalski et al., 2008)

accessing the system. This area i itself has a wide spectrum. It includes the theft of passwords of accessing the computer including logging into the Internet. Such theft could be either by accessing, again authorized or not, into another computer to get information. Once is able to access the computer system, the act of copying, downloading or in any way 'stealing' the information amounts to cyber theft.

c. Spamming

You get up one morning, check your e-mail and your inbox. You spend almost 40 minutes of your reading and deleting them since they are all unsolicited commercial mails. Welcome to the world of cyber spamming! In an effort to impose the message on people who would not otherwise choose to accept it, spam is oversaturating the Internet with numerous copies of its message. Most spam is commercial advertising.[7] 'spam', as used in a newsgroup, means, "the same article (or the same article) posted an unacceptably high number of time to one or more newsgroups". Content is irrelevant. 'Spam' doesn't doesn't mean ads, nor 'abuse'. It doesn't mean 'posts whose content Spam is a funky name for a phenomenon that can be measured objectively: did that post appear X times?[8] E-mail spam targets individual users with direct e-mail m no other form of advertisement does the advertiser pa compared to those to whom the advertisement is aimed. The unsolicited commercial electronic mail may result in costs to recipient, who cannot refuse to accept such mail and who incur co storage of such mail, or for the time spent, reviewing and such mail, or for both. It may impose significant monetary cost on providers of Internet access services, as there is a finite volume of mail that such providers can handle without further investment. of such mail is increasingly and negatively affecting the quality of service provided to customers of Internet access service, and shifting cost from the sender of the advertisement to the provider of Internet and the recipient.

d. Cyber grooming

Practice where individuals build up a passionate association with kids via web-based media stages with the goal of acquiring their trust so they can explicitly mishandle them. This is generally regular with young teen ladies.

e. Child pornography

Child pornography is a serious issue which is emerging in the community and poses an acute threat to the most vulnerable members of the society, that is, children. Unimaginable

[7] Scott Hazen Mueller, "What is Spam ?", at http://spam. whatisspam.html

[8] "The Net Abuse FAQ", available at http://www.cybemothing.org abuse-faq.html#2. 1 (Twenty appears to be the magic number for the figure “x”)

enlargement and development of internet has led to many positive as well as negative effects on children. Internet has no doubt, facilitated innovative study patterns and „day-to-day‟ learning session to enhance the education system both on academic and personal front but at the same time has shown its dark evil side, which cannot be denied. Child abuse is an umbrella term which covers various crimes committed against children. For instance, child trafficking, prostitution, kidnappings and many more. It is significant to note that no country is blessed with immunity in terms of this issue and requires undivided attention at all times. Among all other forms of abuse, child porn is known to be the worst genre. It is so, owing to the fact that it not only causes destruction to the child physically but also tortures him mentally. Pornography has been an arguable topic on the conflict of being right or wrong and pertaining to its existence as it involves adults.[9] As soon as children are embroiled to such an element, it is bound be declared illegal, which is the case in most of the nations. India is known to be one of the largest contributors and consumers of child pornography despite a ban being imposed by the government on sites feeding such content. It is deduced that the situation is alarming as shockingly, almost 35-38 percent of the total pornographic content uploaded online pertains to children.[10] Child pornography is a crime under two pronounced legislations, Information Technology Act, 2000 (ITA) and Indian Penal Code, 1860 (IPC). The Information Technology Bill passed in February 2009 made production, creation and transmission of child pornography illegal and a punishable offence.[11] A striking feature of the bill is that along with other attributes, it makes browsing illicit content pertaining to a child, illegal and prescribed punishment for the first-time offender in such a case can attract five-year sentence as well as a huge fine of Rs. 10 Lakh. Section 67B of the ITA specifically deals with child pornography. According to this section, it is an offence to depict a child engaged in a sexual activity, create text or digital images or advertise or promote any material depicting children in obscene or indecent manner or induce children to online relationship with one or more children.[12] Indian Penal Code does not deal with online obscenity directly but specifies sale, etc of obscene matter to the minors as an

[9] Yukti Lamba, „Why We Need to Look Beyond the Law to Protect Children from Pornography‟ (Youth Ki Awaaz,4 June 2016) accessed 25December 2017.

[10] Shankar Shekhar, „Despite crackdown, India emerges as one of the biggest contributors, consumers of child porn‟ (Mail Today, 6 September 2017) accessed 4January 2018.

[11] Vinod Kapoor and Priya Nagpal, „Child Pornography: A Nuisance‟ (2014) 3 (9) IJSR accessed 4 January 2018.

[12] Prof Nuzhat Parveen Khan and Nida Zainab Naqvi, „Child Pornography in Digital Age and the Law in India-Analysis‟(Eurasia Review, 3 May 2017)

offence.[13] Also, the rationale behind section 292[14] is what drove Section 67 of the ITA to prohibit "obscenity on internet and in electronic form" by the way of amendment of 2008.[15] The Protection of Children from Sexual Offences Act, 2012 (POSCO) is another well thought of legislation, which expressly talks about protecting children from offences pertaining to sexual abuse and pornography in its preamble. It also provides for establishment of Special Courts for such cases and empowers the state to make stringent provisions concerning children. Chapter III of POSCO particularly talks about using a child for pornographic purposes and punishment therefore.[16] Section 15 of the same act provides for punishment for storage of pornographic material involving child making it possession of illicit sexual content pertaining to a child, an offence. It is also pertinent to note that POSCO puts media, studio and photographic facilities under an obligation to report cases of child porn, as and when they come across illegal content online.[17] Test of Obscenity was initially laid down in Regina v. Hicklin.[18] It was stated that, "tendency to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall."

IV. CYBER SAFETY METHOD FOR CHILDREN

In the digital age, children are exposed to a vast amount of technology and the internet, making them vulnerable to cybercrime. Cybercrime includes bullying, harassment, identity theft, fraud, and other online dangers that can harm children's mental and emotional health. As a parent, it's essential to take steps to protect your child from cybercrime. Here are some ways parents can deal with children who are easily vulnerable to cybercrime.

Educate your child about the dangers of the internet:

Educating your child about the risks is the first step in defending them against cybercrime. Discuss with them the dangers of disclosing private information, interacting with strangers online, and obtaining software or files from unauthorised sources. Teach your child to be cautious and use critical thinking skills when interacting with others online.

[13] Sec. 293 Sale, etc., of obscene objects to young person – Whosoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene objects as is referred to in the last preceding section, or offers or attempts so to do shall be punished on first conviction with imprisonment of wither description for a term which may extend to three years, and with fine which may extend to two thousand rupees, and, in the event of second or subsequent conviction, with imprisonment of either description for a term which may extended to seven years, and also with fine which may extended to five thousand rupees.

[14] Sale, etc., of obscene books, etc

[15] Nagpal (n 30) 1785

[16] Section 13 and Section 14

[17] (n 35)

[18] (1868) 2 L.R. 360 (Q.B)

Set rules for internet use:

Establish rules for internet use in your home, such as when and where your child can use the internet and what websites or apps they can access. Be clear about the consequences of breaking the rules and monitor your child's internet use to ensure they are following them.

Use parental controls:

Most devices and apps have parental controls that can help you monitor and restrict your child's internet use. Use these tools to block inappropriate content, set time limits, and monitor your child's online activities.

Encourage open communication:

Encourage your child to talk to you about their online experiences, whether good or bad. Create a safe space for your child to share their concerns, and listen without judgment. Be supportive and provide guidance on how to deal with any negative experiences they may have online.

Monitor your child's social media:

Social media is a common platform for cyberbullying and other online dangers. Monitor your child's social media accounts, and have access to their passwords. Encourage your child to only connect with people they know in real life and avoid sharing personal information online.

Teach your child how to secure their personal information:

Teach your child how to secure their personal information online by having them refrain from sharing sensitive data such as their complete name, address, or phone number. Encourage them to avoid using the same password for many accounts and to generate secure passwords.

Take action if your child is a victim of cybercrime:

Act right away if your child has been a victim of cybercrime. Keep a record of the occurrence and report it to the proper authorities, like the police or the social networking site where it happened. Give your youngster emotional support and, if required, seek expert assistance. Children are vulnerable to cybercrime in the digital age, and parents need to take steps to protect them. Educate your child about the dangers of the internet, set rules for internet use, use parental controls, encourage open communication, monitor your child's social media, teach your child how to protect their personal information, and take action if your child is a victim of cybercrime. By taking these steps, you can help keep your child safe online.

V. GOVERNMENT STEPS TO COUNTER CYBER CRIME

Ministry of Home Affairs dispatched a plan named 'Cyber Crime Prevention against Women and Children (CCPWC)' under which an online National Cyber Crime Reporting Portal, (www.cybercrime.gov.in) was dispatched on 20th September 2018 to empower the general population to report cases relating to child pornography/kid sexual maltreatment material, assault/assault pictures or explicitly express substance. This entryway engages people in general to hold up grievances secretly or through the "Report and Track" alternative. Government also came with legislation to curb the offences. The Personal Data Protection Bill, 2019 in the Parliament in December 2019. The individual information assurance charge looks to ensure the individual information of the individual and foundation of an information insurance expert for the equivalent. Chapter IV of the Personal data protection bill gives arrangements to the handling of individual information and sensitive individual information of the kids. The personal data protection bill was postponed in the parliament in December 2019 and in January the Covid19 pandemic hit the Indian region, so the personal data protection bill is under seclusion. It will be again tabled before the "Parliament" trailed by official consent to turn into an enactment.

VI. CONCLUSION

Giving birth to new technologies is the work of the inventors. Making use of those technologies for more advanced and drastic crimes is the craftwork of the criminals. Controlling such crimes is the result of the interplay of the legislature, executive and judiciary. It is a circle. The society grinds in between this circle with different emotions and reactions. Sometimes, with awe as a new invention springs up, then with distrust when the invention is used for anti-social activities and then with hope as the big brother nails down the criminals with the shackles.

There are many to criticize the IT Act right n to meaningfully interpret it in the light of Indian co circumstances and by understanding the technology itself tailor-made IT jurisprudence in India. Today, India is gearing to be one of the IT super-powers and an efficacious legal support requires to become one.

The ascent of online web exercises in the cutting edge time has welcomed various dangers on the online security of the children. Without tough lawful arrangements, the insurance of such privileges of youngsters appears to be a sunshine dream. Nonetheless, after the increment in online wrongdoings like cyber bullying, phishing, stalking and the data leak, the public authority turned into a little restless and proposed a data protection bill for the assurance of right to the online protection of the individual. On the off chance that bills appear to be too short to even think about possessing the appropriate arrangements for child’s online security assurance, the government ought to have outlined the different, needed, efficient and effective bills in countries like the USA and China.

*****