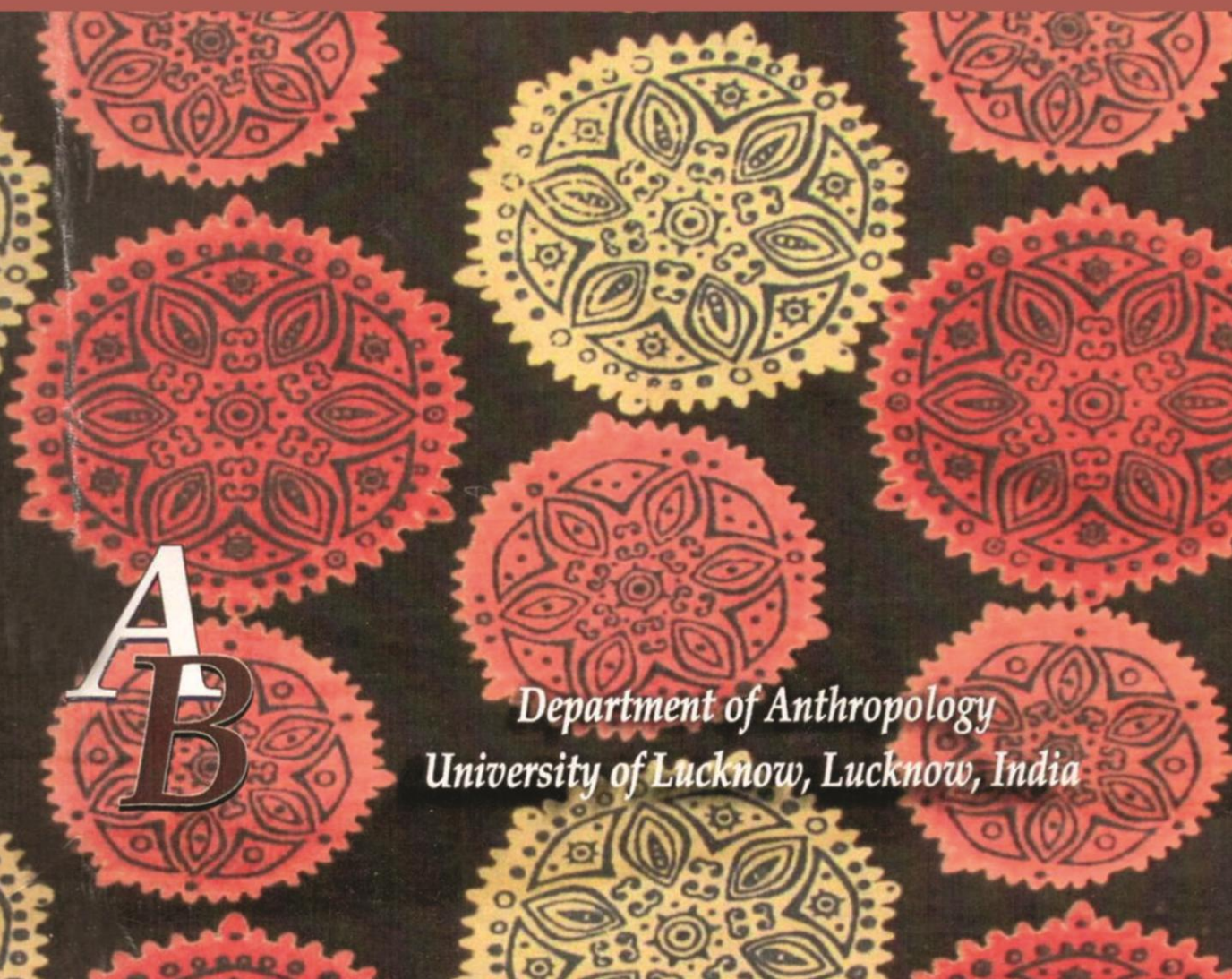
Volume 12, Issue 3
December 2018

ISSN No.:2348-4667

Anthropological Bulletin

a peer reviewed international journal



ISSN: 2348-4667
Anthropological Bulletin
12(3), 64-75, 2018

Understanding Cyber Crimes against Children: A Socio-Legal Approach

Mohd. Ashraf[1] and Shagufta Kahkeshan[2]

ABSTRACT

Cybercrime is a growing issue in the modern world, with computers and the internet facilitating a range of illicit activities. These activities can include hacking, data theft, stalking etc. Cybercrime against children is a growing concern as more children have access to the internet and spend more time online. This type of crime can include various forms of exploitation such as sexual abuse, grooming, and human trafficking. One major issue with cybercrime against children is that it can be difficult to detect and prosecute. Criminals often use the anonymity of the internet to hide their identities and conduct their activities without detection. Additionally, the internet provides a vast and constantly changing landscape, which makes it difficult for law enforcement agencies to keep up with new trends and technologies. Cybercrime against children is a complex and multifaceted problem that requires a comprehensive approach to address. Policies related to cybercrime against children aim to protect children from exploitation and harm, while also holding criminals accountable for their actions. Cybercrime against children presents a unique challenge to police agencies, policy makers, and internet intermediaries as they must protect the most vulnerable users. This paper will explore the various aspects of cybercrime against children, including the causes, effects, and the ways in which society can address the problem.

KEYWORDS- Cybercrime, Child pornography, Cyber bullying, Online grooming.

I. INTRODUCTION – CYBER CRIME AGAINST CHILDREN

The advancement of technology has drastically altered our way of life. In the past, computers were considered a luxury or extravagance and people relied on traditional forms of media for news and information. However, now computers have become a staple in various settings such as businesses, homes, schools, and libraries. The internet offers immediate access to a vast array of information and services including news, shopping, banking, and entertainment. The internet has also made communication much more convenient through the use of chat rooms and emails.

The proliferation of digital technology has had a significant impact on the lives of children and adolescents, as the internet, devices such as tablets and smartphones, social media platforms, and messaging apps have become an integral part of their daily lives. These

[1] Professor, Department of Law, Aligarh Muslim University, India.
[2] LLM Student, Department of law, Aligarh Muslim University, India

technologies have transformed their educational experiences, the way they form and maintain friendships, how they spend their leisure time, and their engagement with society at large. About one out of three minor under 18 year of age are internet users and about 71 per cent of 15 to 24 age group are internet users.[3] However, there exists a significant digital divide, with 346 million youth not having access to these technologies, particularly in Africa where 60% of adolescents are not connected compared to 4% in Europe. This lack of access to digital technology can prevent these young people from having access to educational, job training, and employment opportunities, which can help break intergenerational cycles of poverty and access to information sources that can help protect their health, safety, and rights.[4]

While technology has improved productivity and provided new opportunities for education and recreation, it has also been utilized by criminals for nefarious purposes. The internet has made it easier for predators to target children for committing crimes like child pornography, stalking, and sexual exploitation. The nature of internet crimes poses great challenges for investigative agencies and ISPs in terms of investigations, evidence collection, offender identification and apprehension, and assisting child victims and their families. Internet have opened up a new realm of opportunities for children to learn and entertainment. However, this realm also comes with its own set of risks, where children can become victims of cybercrime.[5]

The digital age has brought about various opportunities; however, it also presents a wide range of dangers and harms. One such harm is the escalation of child sexual abuse and exploitation, as digital technologies have provided child sex offenders with increased access to children through unprotected social media profiles and online gaming forums. Furthermore, advancements in technology have enabled individuals and criminal organizations to evade detection by utilizing encrypted platforms and creating false identities, allowing them to target multiple victims at once. Additionally, young people are not only at risk from adult exploitation, but they can also become victim to peer exploitation through the distribution of sexual or intimate photos without consent. Furthermore, digital technologies have expanded the scope of bullying, as cyberbullying now allows bullies to harm and humiliate their victims with a simple click of a button. Words and images posted online that are intended to cause harm are also difficult to delete, increasing the risk of re-victimization.[6]

With easy access, new forms of exploitation are emerging, such as the creation of custom-made child sexual abuse materials, where offenders can order materials tailored to their specific preferences, including the age, race, and sexual conduct of the victims, as well as the setting and fictional scenarios involved.

II. VULNERABILITY OF CHILDREN AS VICTIMS OF CYBER CRIME

The anonymity afforded by the internet serves as a facilitator for individuals engaging in predatory behaviour, enabling them to perpetrate criminal conduct against minors who, due to their youthful nature, may be trusting, uninformed, inquisitive, and seeking attention and

---

[3]UNICEF, State of the World's Children 2017: Children in a Digital World Report, available at https://www.unicef.org/reports/state-worlds-children-2017

[4] Growing in the Digital world: Benefits and risks, available at: https://www.youthlead.org/resources/growing-digital-world-benefits-and-risks

[5]Shobhna Jeet, "Cybercrimes against women in India: Information Technology Act, 2000", 47 *Elixir International Journal* 8891-8895 (2012).

[6]The Lancet Child & Adolescent Health, Growing Up in A Digital World: Benefits and Risks, 2018, Available at: https://gdc.unicef.org/resource/growing-digital-world-benefits-and-risks

affection. Regrettably, such minors are often deemed as less credible in legal proceedings, resulting in perpetrators evading accountability for their actions. Thus, making them vulnerable to cyber-crimes.

The methodology employed by perpetrators, regardless of whether the abuse occurs physically or through the cyberspace, is consistent, characterized by the utilization of information for the purpose of identifying and targeting child victims. This may involve the establishment of an online relationship with a minor, through the sharing of common interests and activities, which may ultimately lead to the exchange of gifts and photographs. Similarly to traditional predators, those operating online will often invest a significant amount of time in cultivating a relationship with a child, prior to committing any criminal acts. [7] The perpetrator's intent is to establish a level of trust with the child victim, which serves to facilitate the perpetrator's ultimate goal. Although any child may be susceptible to exploitation and harassment on the internet, certain factors may render certain children more vulnerable to such conduct.

Older minors tend to be at increased risk due to their tendency to utilize the internet unsupervised and their inclination to involve in internet conversation of a private nature. Some victims may inadvertently become involved in such activities through their participation in chat rooms, email exchanges, and the sharing of photographs online. Adolescents who are struggling with emotional or behavioural issues, such as rebellion or a desire for independence, may also be particularly susceptible to exploitation by internet predators. Additionally, emotionally or mentally vulnerable youth, who may be navigating issues related to their sexual identity, may also be at a heightened risk of victimization. Such individuals may be inclined to engage in conversations that, although appearing innocent and harmless, may gradually lead to sexually explicit conduct.[8]

III. CHARACTERISTICS AND FACTORS OF CYBERCRIMES AGAINST CHILDREN

There are various distinct characteristics that differentiate internet crimes committed against children from other crimes:

(i) Physical contact between the perpetrator and the child is not necessary for a crime to occur or for the child to become a victim, as innocent images or photographs of children can be digitally manipulated and distributed as pornographic material on cyber space without child's knowledge.

(ii) The utilization of the internet enables the perpetuation and reiteration of abuse towards a minor, which can persist for extended durations, frequently without the cognizance of the victim. Once an image of a child is uploaded onto the internet, it may remain accessible indefinitely.

(iii) These offenses frequently transcend geographical limitations, encompassing numerous victims from various demographics, regions, and nations. The location of the child is not a significant factor for offenders who prey on victims via the internet, and many of these matters require the participation of law enforcement agencies at the local, state, and international level across multiple jurisdictions.

(iv) A large number of victims of crimes committed through the internet do not report it or are not aware that they have been targeted. Unlike minors who have been subject to physical or sexual abuse, who may divulge the abuse to a reliable adult, victims of cybercrime may remain unidentified until their participation is exposed during an inquiry by law

[7] J.P.S. Sirohi, *Criminology & Penology* 347 (Allahabad Law Agency,7th edition, 2014).

[8] Karnika Seth, "*Overview of Laws against online child sex abuse in India, U.K, U.S*", 2(12) International Journal of Research (2015), available at: http://internationaljournalofresearch.org

enforcement. The supposed anonymity of internet-based actions can foster a false sense of protection and confidentiality for both the perpetrator and the victim.

When it comes to cyber crimes against children, there are a number of underlying factors that contribute to the vulnerability of children to exploitation. These include:
(i) Socio-economic status, where children from low-income backgrounds or those facing gender inequality may be at a higher risk of falling prey to online predators.
(ii) Racism and discrimination, where marginalized children may be more vulnerable due to the lack of access to resources and support systems.
(iii) Migration, where children who have recently moved to a new country may be more susceptible to online predators due to their lack of familiarity with local laws and customs.
(iv) Social isolation, where children who are lonely or detached may be more likely to engage with strangers online, making them more vulnerable to exploitation.
(v) Sexual orientation, where LGBTQ+ children may be at a higher risk due to discrimination and prejudice they may face in society.
(vi) Abusive and unstable family environments, where children who have experienced abuse or neglect may be more likely to be targeted by predators.
(vii) Inadequate legal frameworks, policies and protective mechanisms, where a lack of effective laws and regulations may leave children more vulnerable to online exploitation.
(viii) Limited digital literacy, where children with less knowledge of the internet and its potential dangers may be more likely to fall prey to predators.
(ix) Characteristics and motivations of offenders, where certain individuals may be predisposed to committing cyber crimes against children.
(x) Technological expertise, where those with advanced technical skills may be better equipped to exploit children online.
(xi) Organized criminal groups, where well-established criminal networks may target children online for sexual exploitation and other forms of abuse.[9]

IV. CYBER CRIMES AGAINST CHILDREN

Offenders engage in a wide range of cyber crimes against children, including but not limited to, child abuse, exploitation, cyberbullying, child pornography, and exposure to harmful content. Young children and teenagers are often targeted due to their trustworthiness, naivety, curiosity, and desire for attention and affection. For instance, an offender may establish a social media friendship with a child by sharing common interests and activities, which could result in the exchange of gifts and photographs. The offender aims to gain the child's trust in order to achieve their ultimate goal. Some examples of cyber crimes against children include online grooming, where predators use social media and other platforms to establish relationships with children, and then manipulate them into sending explicit photos or meeting in person; sextortion, where predators threaten to expose sexually explicit photos or videos of a child unless they comply with their demands; and live streaming of abuse, where predators use live streaming platforms to sexually exploit children in real time.In order to combat these crimes, the government has implemented laws, initiatives, and policies to ensure that all citizens have access to a safe, secure, and transparent internet.

Cybercrime against children can take many forms, some of which include:
(a) Child pornography: Child pornography involves the creation, distribution, and possession of sexually explicit materials that depict children. These materials can include

[9] V. Paranjape, *Cyber Crimes & Law* (Central Law Agency, 1St edition, 2010).

images, videos,[10], sound recordings,[11] or illustrations of children in sexually suggestive or explicit situations. Child pornography is often referred to as "child sexual abuse images" as it involves the abuse of children. Additionally, it can also be created through computer-generated images, which are referred to as "simulated child pornography", "virtual child pornography", "non-photographic child pornography" or "pseudo-photographic child pornography", These images depict virtual or simulated children, which means that the children depicted in the images are not real.[12]

(b) Online grooming: This refers to the process of gaining the trust of a child, usually through social media or other online platforms, in order to exploit them sexually or emotionally. Online grooming, also known as internet grooming, can be challenging to identify as it often takes place when a child is using their computer at home. Perpetrators of this crime often instruct their victims not to disclose their conduct to others. Though, there can be signs that a child is being groomed by a cyber offender, such as an increase in internet usage, being private and secret during their activities, quickly changing displaying screens or closing device when a parent is nearby, using sexually explicit language they would not be expected to know, and showing sudden changes in emotional behaviour.

(c) Online Cheating: This refers to using the internet to obtain money or property by deceiving a child.

(d) Cyberstalking: This refers to the act of repeatedly and persistently harassing, threatening or intimidating a child through the internet. Cyberstalking is a criminal offense in which an individual repeatedly attempts to contact another person through various digital means, creating a sense of fear or threat in the mind of the victim. This crime is often perpetrated against women and children.[13]

(e) Cyberbullying: This refers to the use of technology to harass, humiliate, or intimidate a child that takes place online causing embarrassment or distress to the targeted person.It is a type of bullying that can take place through any device that can access the internet, such as computers, mobile devices, gaming consoles and cellphones. It does not require the bully to be in physical proximity of the victim.[14] This type of bullying is particularly prevalent among children as it often extends from bullying that occurs within schools.[15]

(f) Hacking: This refers to unauthorized access to a child's computer, email or social media account in order to steal personal information or harm the child.

---

[10]Alisdair A. Gillespie, *Child Pornography: Law and Policy* 21(Routledge, 1st edition, 2012)

[11]Yaman Akdeniz, *Internet child pornography and the law: National and international responses*, (Routledge, 1st edition,2016).

[12] Hadeel Al-Alosi, *The Criminalisation of Fantasy Material: Law and Sexually Explicit Representations of Fictional Children* (Routledge Publication, 1st edition, 2018).

[13] Cyberstalking and Its Impact on Vulnerable Group: Women and Minors, available at: https://www.legalserviceindia.com/legal/article-8829-cyberstalking-and-its-impact-on-vulnerable-group-women-and-minors.html#:~:text=In%20simple%20layman%20terms%20%22Cyberstalking,the%20women%20and%20the%20minors

[14]Robert Slonje, & Peter K Smith, "Cyber-bullying: Another main type of bullying?" 49(2) *Scandinavian Journal of Psychology* 147-154 (2008).

[15] Tanya Beran& Qing Li, "The Relationship between Cyber-bullying and School Bullying" 1(2) *The Journal of Student Well-being* 15-33 (2007).

(g) Online child trafficking: This refers to the use of the internet to lure children into sexual exploitation or forced labour.

(h) Online extortion: This refers to the use of the internet to threaten or blackmail a child into giving up money or personal information.

(i) Online sexual harassment: This refers to unwanted sexual advances or sexual harassment that occurs online or through technology.

(j) Violation of privacy: This refers to the unauthorized access or collecting of personal information of a child, such as tracking their location, accessing their messages, or monitoring their activities on social media.
It's important to note that these forms of cybercrime are not mutually exclusive and may overlap in some cases, and the impact of these crimes on children can be severe and long-lasting.

V. LEGAL FRAMEWORK AND DEVELOPMENT OF MEASURES TO COMBAT CYBER CRIMES AGAINST CHILDREN

The power to enforce and investigate such cyber-crimes falls as a state matter under 7th schedule of constitution as they fall under the heads of "police" and "public order". However, both centre and state governments have been working together to fight the menace, and they have been working towards capacity building programmes. According to data from the National Crime Records Bureau (NCRB), in the year of 2017[16] about 88 cases of cyber-crime against children were reported respectively, as per the National Crime Records Bureau (NCRB) data.

There have been numerous measures to protect children from cyber-crimes. The "Information Technology (IT) Act, 2000"[17] (Herein after as "IT ACT"), is a legislation that governs cybercrime in India. "The Information Technology Amendment Act 2008" further clarified the definition of the term "communication device" in Section 2(1) (ha), which now includes mobile phones, iPads, tablets, laptops, and computers.

"Section 67B of the Act deals specifically with the publishing, transferring, or accessing of internet content containing child sexual abuse." It includes child pornography, child grooming and exploitation. This section of the Act imposes severe penalties, including imprisonment upto 5 years and/or fines, for individuals found guilty of committing such offenses. This is intended to serve as a deterrent to individuals who may be inclined to engage in such activities, and to provide a legal framework for the prosecution of such crimes.

Further, there are other provisions which are not specifically made for children but they applicable to them like section 66-E provides punishment for violation of privacy by transmitting and publishing pictures and videos without the consent. Section 66 read along with section 43 provides for various offences such as data theft, hacking, damaging computer of child etc. Further, section67 provides for "punishment for publishing or transmitting obscene material in electronic form" and 67A provides for "punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form." Lastly, there is identity theft under section 66-C of the IT Act.

---

[16] https:// www.Indiastat.com/table/incidence-of-crime-committed-under-cyber-crimes/state-type-wise-number-cyber-crimes-against-childr/1432325

[17](Act 21 of 2000), enforced on 17th Oct,2000.

The Protection of Children from Sexual Offenses Act, 2012 (Herein after as "POCSO Act of 2012") is a crucial law that specifically deals with sexual crimes against children. It makes it a crime to engage in cyber activities such as child pornography, cyberbullying, cyberstalking, hacking, identity theft, online child trafficking, online extortion, sexual harassment, and violation of privacy against children. In particular, Section 11 of the POCSO Act defines instances of sexual harassment involving electronic media, such as showing pornographic material to a child on electronic media, constantly contacting a child through electronic media, threatening a child through electronic means to engage in sexual acts, luring a child for pornographic purposes. It also includes the law of online grooming r/w 67-B IT Act, 2000 and 366-A, I.P.C.

Section 12 of the POCSO Act provides penalties for sexual harassment, which includes imprisonment for a term of up to three years and a fine. Section 13 of the POCSO Act prohibits the use of children for pornographic purposes through electronic media, including the display of sexual organs of a child and the display of a child engaged in sexual acts. Penalties for violating this section include imprisonment for a minimum of five years and a fine, with harsher penalties for repeat offenses. Section 15 of the Act criminalizes the storage and possession of pornographic material involving children, with punishments including fines and imprisonment. Section 16 of the Act also provides penalties for abetting any of the above offenses.

In addition to the POCSO Act, the Indian Penal Code also applies to offenses such as criminal intimidation, hate speech, and defamation committed online, including Section 153A of IPC which pertains to hate speech, Section 292 of the code prohibits the possession, sale, and distribution of obscene material. While these provisions are not specifically directed towards offenses committed against children, they can be applied in such cases. sections 354A and 354D of the Indian Penal Code provide for penalties for cyber harassment and cyber stalking against women. The other provisions of law for cyber stalking are in section 72 of the IT Act r/w 354-D or 354-C of IPC.

The provisions which were added by 2013 amendment are for female minors only and they are not gender neutral. Further, Section 419 of IPC which pertains to cheating by impersonation. The law in substance for cyber bullying is in Indian Penal Code are embodied in section 499, 500 which pertains to defamation and Section 503, 507 and 509 which pertains to criminal intimidation. We can see that Indian framework has scattered legal provisions, and most of the provisions do not define certain crimes and they have to gathered from various laws. Thus, the scheme of prosecution is not exhaustive and effective per se as compared to western laws.

If we look into the practices of other jurisdictions, there have been stricter laws and provisions to curb cyber-crimes against children. For Instance, in U.S.A, Social networking websites under various agreements with States are required to protect minors who use their platforms by the following ways such as making age restriction sections, restriction of change in age by users, warning to minors for not giving any private information, removal of sex predators from its websites.

To restrain child grooming, and sexual abuse, some States have made restriction to sex offenders to even access social media[18], and sex offenders had to share username, email addresses and in some cases passwords by sex offenders to authorities.[19] These laws are

[18] ILLIONIS banned the access of sex offenders to access social media in 2009 vide House Bill 1314

[19] H.R. 34, 2008 Gen. Sess. (Utah 2008), UTAH CODE ANN. § 77-27-21.5(12) (2008); Georgia has a similar law as well; S.B. 474, 2007-2008 Leg., Gen. Assem. (Ga. 2008), GA. CODE Ann. § 42-l-1 (2009).

problematic as they transgress to the fundamental rights of speech and access to internet and they have been subject to litigation.[20] For the same reason, these laws are not possible for legislation in India. However, we can legislate special provisions to make effective prosecution and detection of the crimes.

As far child grooming is concerned, there is no clear law in India. For instance, in U.K Sexual Offences Act, 2003, section 15 provides meeting a minor under 16 years of age pursuant to a "sexual grooming" is punishable up to 10 years. Similarly, in U.S.A, title 18 of the U.S Code punishes "persuading, inducing and enticing a minor to travel and engage for sexual activity" has been made punishable. On the other side, there is no clear definition in India. A committee of the Upper House has stated to include child grooming as a separate provision in POCSO Act to bring in parity with international laws and practices. The committee recommend the following definition under section 11 of the POCSO Act as follows: -

"*Section 11 (vii) of the POCSO Act; knowingly persuades, coerces, entices, grooms, communicates, arranges a meeting with a child for oneself or another person and/or meets with a child with the intent of sexually abusing the child, and even if the actor thinks he/she is communicating with a child but is actually talking to an adult.*"

This definition will help in higher reporting of cases, and guidebook for law enforcement agencies and Courts. Therefore, there is a need for desired separate provision for online grooming in India.

Similarly, India does not have a separate law which specifically defines cyber- bullying. There are two issues while dealing with cyber- bullying i.e., firstly, in most cases of cyber bullying, the accused is a peer of the child who happens to be a minor himself. Therefore, the remedy is to be availed through "Anti-Bullying committees" made by schools such as "CBSE Guidelines for prevention of Bullying and Ragging in Schools" or the report may be made to a cyber cell who may further report to the Juvenile Justice Board which may inquire and take action.The second issue is to give a precise a definition to cyber-bullying. As such law would have potential of misuse and threaten free speech. The standard to determine the annoyance, harassment and abuse would only be possible with deliberate and concise attempt to define it.

As far the solution is concerned for cyber-bullying or any other objectionable cyber-content, most of the social media websites have a regulating reporting mechanism. However, such mechanism is discretionary according to the policy of the websites. There is a need to increase the liability of social media sites, intermediaries and search engines to remove such content by notice as soon as possible. "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" provides additional protections for users of intermediaries, such as social media platforms, and hold these intermediaries accountable for ensuring the safety and security of their users. These rules mandate that intermediaries establish a robust grievance redressal process, including prompt resolution of complaints, to address any issues related to safety and security. Additionally, intermediaries must inform users of their terms and conditions, which must include a "warning against hosting, displaying, uploading, altering, publishing, transmitting, updating, or sharing any information that is, among other things, harmful, defamatory, obscene, invades another's privacy, harms children in any way, or is otherwise illegal". This is intended to provide users with more control over their safety and to hold intermediaries accountable for ensuring that

[20]Charlotte Chang,"*Internet Safety Survey: Who Will Protect the Children?"*, 25(1) Berkeley Technology Law 501-27 (2010).

their platforms are not used to spread harmful or illegal content. However, hefty fines need to be put upon intermediaries upon failure to remove in a timely manner.

Lastly, for co-ordination of various agencies, the Indian Cyber Crime Coordination Centre (I4C) is a government-established body that is tasked with coordinating the efforts of various law enforcement agencies (LEAs) in the fight against cybercrime. This centre is located under the Ministry of Home Affairs, and its goal is to provide a structured and organized system for combatting cybercrime in India. By centralizing resources and coordinating efforts, the I4C aims to create a more effective and efficient response to cybercrime, and to ensure that all relevant agencies are working together to combat these crimes in a thorough and coordinated manner. There is a need to develop co-ordination in the lines of Internet Crimes Against Children (ICAC) task programme of U.S.A for an effective response against children crimes. This will enhance "investigative, forensic, technical, training and education dimensions" of detection and prosecution cyber-crimes against children.

VI. STEPS TAKEN FOR EDUCATING ABOUT CYBER CRIMES

The most significant way to fight against cyber-crimes is to educate children for two reasons. Firstly, it provides a preventive approach instead of a reactive approach. Secondly, it is not easier for the authorities to detect beforehand cyber criminals in a vast country. Therefore, it requires a greater focus along with enforcement and prosecution measures. There have been a number of steps taken for educating children against cybercrimes and creating a safer cyber friendly environment. The Ministry of Women and Child Development, in an effort to address and prevent issues related to the safety and security of women and young children utilizing online platforms, brought the matter to the attention of the "Ministries of Home Affairs, Electronics and Information Technology, and Education". Specifically, the Ministry of Education was requested to provide direction to the Central Board of Secondary Education to incorporate suitable cyber safety material in the school curriculum for children, and to encourage the State Governments to similarly integrate this content into their own school board curriculums in order to equip children with the necessary knowledge to navigate the online world safely.

The "National Policy of ICT in Schools, 2012 and the National Cyber Security Policy, 2013" also aim to safeguard children from online risks. The former aims to improve and enhance school education through the use of information and communication technology while the latter deals with comprehensive efforts to enhance cyber security in the country.

In 2017, the "Central Board of Secondary Education (CBSE)" issued guidelines for the safe and secure use of the internet in schools. These guidelines instruct schools to "develop comprehensive security policies and implement efficient firewalls, filtering, and monitoring software on all computers." This is intended to ensure that students have access to the internet while also being protected from any potential online threats, such as cyberbullying, online harassment, or exposure to inappropriate content. The CBSE guidelines aim to empower schools with the necessary tools and knowledge to protect students while they are using the internet, and to create a safer online environment for students.[21] For reporting mechanism, National Cyber Crime Reporting Portal has been constituted for crimes against women and children along with various toll-free numbers. Social media accounts of cyber dost, FM radio shows and handbook literature has been made for awareness.[22]

---

[21]Ministry of Women and Child Development, Steps to tackle Cyber Crime against Children, PIB Delhi, available at https://pib.gov.in/PressReleasePage.aspx?PRID=1706002

[22] Ibid.

Further, for safer internet access points and environment, the IT (Guidelines for cybercafe) rules, 2011 had made provisions for Cybercafes. For accessing internet, they must require the person to submit their identity proof to access from the cyber café as it helps to ascertain identity of the users. Further, they must use filtering software which will prevent access to pornographic websites and other obscene content. Additionally, they should display clear "signage prohibiting access to pornographic websites, copying or downloading any content prohibited under the IT Act" as well as any other websites that are prohibited by the act itself. This is important because it ensures that all visitors – especially minors - are aware of what type of content is off limits within these establishments and helps them avoid witnessing anything inappropriate or illegal online activity during their visit.

VII. CONCLUSION AND RECOMMENDATIONS

To protect children from cybercrime, it is important to take both preventative measures and educate them on how to stay safe online. Parents and guardians play a crucial role in this by teaching children about the dangers of exploitation, pornography, violence, and other issues that may arise on the internet. They should also monitor their children's internet use and consider using parental control features offered by commercial online services. The following measures are required to combat cyber-crimes against children: -

(i) Consolidation of Cyber Crimes against children by making a special law to address the crimes. This will help in effective detection of crimes and their prosecution by police and Courts. If legislating a special law is not possible in the near future, defining the crimes should be the priority.
(ii) Creation of a task force to develop co-ordination in the lines of Internet Crimes Against Children (ICAC) task programme of U.S.A for an effective response against children's crimes. This will enhance "investigative, forensic, technical, training and education dimensions" of detection and prosecution cyber-crimes against children.
(iii) Collection of data and studies on a regular basis to determine the scale of cyber crimes against children. Since in most cases, the crimes go unreported and undetected. The second and third suggestion is only possible by allocating larger funds.
(iv) Introduction of hefty fines upon intermediaries in failure to remove objectionable content in the defined timeline. This would give a speedy mechanism to deal with cyber crimes and the intermediaries may develop a self-reporting AI based mechanism to filter out potential cyber-crimes.
(v) It is important to educate children on digital literacy, enhance their digital skills and increase competency of teachers, and provide workshops and lectures on online safety at schools. Children should be taught to inform their parents immediately if they come across anything scary or threatening online, and they should not share personal information such as their name, address, telephone number, passwords, school name, parent's name or any private information.
(vi) Children should also be taught about tolerance and empathy in the digital world through socio-emotional learning, and parents, teachers, and guardians should serve as positive digital role models.
(vii) Additionally, parents should monitor and control their children's access to websites, networks, and social media platforms that may distribute harmful or offensive materials. It is also important to be cautious when using social networking sites, and to limit the amount of personal information shared. Use of strong passwords, regular upgrades of anti-virus software and not sharing personal information about friends and family members are also important.
(viii) It is also important to safeguard children's privacy, personal information, and reputation. Overall, a comprehensive approach that includes education and awareness,

parental involvement, and proactive regulation is necessary to effectively protect children from cybercrimes.

(ix) In addition, parents, teachers, guardians, and mentors can serve as positive digital role models for children by preventing or blocking access to websites, networks, and services that distribute harmful or offensive materials, such as pornography and dangerous online games. They should also access parental locks for various online applications and safeguard and protect children's privacy, personal information, and reputation.

(x) It is important to note that certain factors make children more vulnerable to cybercrime, including gender, race, socio-economic upbringing, age etc. Therefore, it is essential to provide education and awareness for children and parents to understand how sex offenders work and interest in the devices and media they provide access to their children, teaching them on their use and the likely effects of reckless online behaviour.

List of Abbreviations

- IPC –Indian Penal Code
- N.C.R.B –National Crime Record Bureau
- IT ACT - Information Technology Act
- POCSO Act- The Protection of Children from Sexual Offenses Act
- LEAs- Law enforcement agencies
- ICAC- Internet Crimes Against Children

Bibliography

A: BOOKS

Alisdair A. Gillespie, Child Pornography: Law and Policy,Routledge-Cavendish, 1st edition, 2012.

Hadeel Al-Alosi, The Criminalisation of Fantasy Material: Law and Sexually Explicit Representations of Fictional Children, Routledge Publication, 1st edition, 2018.

J.P.S. Sirohi, Criminology & Penology, Allahabad Law Agency,7th edition, 2014.

V. Paranjape, Cyber Crimes & Law, Central Law Agency, 1st edition, 2010.

Yaman Akdeniz, Internet child pornography and the law: National and international responses,Routledge, 1st edition,2016.

B: ARTICLES/JOURNALS

Charlotte Chang, "*Internet Safety Survey: Who Will Protect the Children?"*, Berkeley Technology Law (2010).

Karnika Seth, "*Overview of Laws against online child sex abuse in India, U.K, U.S*", International Journal of Research (2015), available at: http://internationaljournalofresearch.org.

Robert Slonje, & Peter K Smith, "Cyber-bullying: Another main type of bullying?" Scandinavian Journal of Psychology (2008).

Shobhna Jeet, "Cybercrimes against women in India: Information Technology Act, 2000", Elixir International Journal (2012).

Tanya Beran& Qing Li, "The Relationship between Cyber-bullying and School Bullying" *The Journal of Student Well-being* (2007).

C: WEBSITES

Cyberstalking and Its Impact on Vulnerable Group: Women and Minors, available at: https://www.legalserviceindia.com/legal/article-8829-cyberstalking-and-its-impact-on-vulnerable-group-women-and-minors.html#:~:text=In%20simple%20layman%20terms%20%22Cyberstalking,the%20women%20and%20the%20minors

Growing in the Digital world: Benefits and risks, available at: https://www.youthlead.org/resources/growing-digital-world-benefits-and-risks

Ministry of Women and Child Development, Steps to tackle Cyber Crime against Children, PIB Delhi, available at https://pib.gov.in/PressReleasePage.aspx?PRID=1706002

The Lancet Child & Adolescent Health, Growing Up in A Digital World: Benefits and Risks, 2018, Available at: https://gdc.unicef.org/resource/growing-digital-world-benefits-and-risks

UNICEF, State of the World's Children 2017: Children in a Digital World Report, available at https://www.unicef.org/reports/state-worlds-children-2017

www.Indiastat.com/table/incidence-of-crime-committed-under-cyber-crimes/state-type-wise-number-cyber-crimes-against-childr/1432325

*****