The Protection of Children from Cyber Crimes in India

Ms. Jaya Thapa

Assistant Professor (Contract basis), Dept. of Laws, GNDU, RC, Jalandhar

ABSTRACT

Information and communication technology has become an integral part of modern civilization, permeating every aspect of our daily lives. The proliferation of digital technologies has brought about positive as well as negative changes in human life. Especially, Internet has affected the rights of children globally. Information Communication Technology has provided new tools to develop a child not only educationally but also different aspects of his personality but there are also some negative impacts on children in the form of different digital violence against them. Cybercrimes against children have become a pervasive issue globally, encompassing a wide range of malicious activities such as cyberbullying, online harassment, grooming, sextortion, child sexual exploitation etc. The paramount importance should be given to safeguard the Children and adolescents of our country in cyberspace.

This paper provides a comprehensive analysis of cybercrimes in India, examining the various types of offenses, legislative frameworks, and judicial approaches aimed at protecting children in the digital age.

Keywords: Children, Cyberspace, Cybercrime.

1. INTRODUCTION

In today's world, social media, financial transactions, mobile transactions, and other forms of communication and connection rely entirely on digital space. As innovation in technical growth leads to an increasing reliance on the internet. The internet is widely used in the modern world for a wide range of purposes that make people's lives more pleasant and enjoyable. Every industry, including the railway, education, research, space, communications, health, banking, aviation, social media, and others, is completely dominated by the internet or gadgets with internet access. Every innovation or technology changes the lives with positivity but it also has some bad effects also.

For everyone around the world, cybercrime is a new kind of criminality. According to the Information Technology Act, it is any illegal behaviour conducted through or on computers, the internet, or other technologies. Technically proficient criminals use the internet to execute a variety of unlawful acts. Using a more expansive definition, cybercrime may be defined as any unlawful conduct in which a computer or the internet is used as a tool, a target, or both. Because of the misuse of the growing reliance on computers in modern life, cybercrime is an unchecked evil. The usage of computers and related technologies in daily life is expanding quickly and has turned into a need that makes users' convenience easier. It is an unlimited, unquantifiable medium. Cyberstalking, cyberterrorism, email spoofing, email bombing, cyberpornography, cyberdefamation, and other recently developed cybercrimes are some examples. If they are carried out using a computer or the Internet, several traditional crimes may also be classified as
cybercrimes.\textsuperscript{1} Concern and difficulty are growing from our growing reliance on the digital world for work, entertainment, socialisation, finance, and communication. The offences or illegal activities which take place on or using the one or more components or medium of the internet are known as cybercrimes. Any criminal offence on web using the medium of internet such as email, chat, websites, apps etc to conduct unlawful financial transaction, harassment, online child sexual abuses, pornography, cyber terrorism, stealing or leaking personal information, hateful posts for violence or riots. Cybercrime is a broad category of illegal activity that is becoming a greater hazard and source of issues for the modern world. The number of online crimes and legal transgressions in the digital age is rising daily. The cybercrime can be categorized into two such as ‘property crimes’ and ‘crimes against person’. The following fall under the category of crimes against people: cyberstalking, cyberbullying, child pornography, leaking private images or videos, illicit transactions, identity theft, scams, fraud, and copyright infringement.\textsuperscript{2} Cyber-crimes against children globally have been a growing concern, and India is no exception. The proliferation of digital technologies and increased internet access among children have unfortunately provided more opportunities for cyber predators to exploit vulnerabilities and target minors for various forms of abuse and exploitation. According to the NCRB data, there were 1,823 instances of cybercrimes against minors in 2022 compared to 1,376 the year before. Among these offences are 416 other cyber-related offences, 158 instances of cyberstalking and bullying, and 1,171 instances of cyberpornography or the distribution of offensive content.\textsuperscript{3}

2. IMPACT ON CHILDREN ON CYBERSPACE
Cyberspace has a complex effect on children, having both beneficial and adverse effects. While the internet offers numerous educational, social, and entertainment opportunities, it also exposes children to various risks and challenges. Here are some key aspects of the impact of cyberspace on children:

Positive Impact:
1. **Access to Information and Education**: Cyberspace provides children with vast resources and information, enabling them to access educational materials, online courses, and academic resources. This facilitates self-directed learning and supports academic achievement.\textsuperscript{4}
2. **Social Connectivity**: Children can connect with peers, family members, and communities globally through social media platforms, messaging apps, and online forums. This fosters social interaction, friendships, and cultural exchange, promoting social development and a sense of belonging.
3. **Creativity and Expression**: Online platforms offer opportunities for children to express themselves creatively through art, writing, music, and other forms of digital content creation. They can share their talents, ideas, and perspectives with a wide audience, enhancing self-confidence and creativity.

\textsuperscript{1} Osman Goni, “Introduction to Cyber Crime” 3 International Journal of Engineering and Artificial Intelligence 9 (2022).
\textsuperscript{4} Dr. Dalbeer Lal, “Protecting the Child from the Evil Effects of the Digital Age” 10 *International Journal of Creative Research Thoughts (IJCRT)* e74 (2022).
4. **Entertainment and Recreation**: Cyberspace offers a plethora of entertainment options, including online games, streaming services, and digital media content. These activities provide relaxation, enjoyment, and opportunities for leisure and recreation.

5. **Learning and Skill Development**: Interactive educational games, simulations, and virtual learning environments help children develop critical thinking, problem-solving, and digital literacy skills. They can learn coding, programming, and STEM subjects in engaging and interactive ways.\(^5\)

### Negative Impact:

1. **Cyberbullying and Harassment**: Children are susceptible to online abuse, trolling, and cyberbullying, all of which can have detrimental effects on their mental and emotional health. Negative interactions on social media platforms or messaging apps can lead to anxiety, depression, and low self-esteem.

2. **Exposure to Inappropriate Content**: The internet exposes children to age-inappropriate, violent, or sexually explicit content, including pornography, hate speech, and graphic imagery. Exposure to such content can desensitize children, distort their perceptions, and pose risks to their mental and emotional well-being.

3. **Privacy and Security Risks**: Children may unknowingly share personal information online, leading to privacy breaches, identity theft, and cyberstalking. They may fall victim to online scams, phishing attacks, or malicious software that compromise their digital security and safety.

4. **Addiction and Screen Time**: Excessive screen time and internet use can contribute to addiction, sedentary behavior, and sleep disturbances among children. Spending too much time online may affect their physical health, social interactions, and academic performance.

5. **Online Predators and Grooming**: Children may encounter online predators who use deceptive tactics to groom and exploit them for sexual purposes. This can lead to instances of online sexual abuse, sextortion, or trafficking, posing significant risks to their safety and well-being.

6. **Digital Divide**: Disparities in internet access, digital literacy, and technological resources contribute to a digital divide among children from different socioeconomic backgrounds. Children lacking access to cyberspace may face inequalities in education, opportunities, and social inclusion.

Overall, while cyberspace offers numerous benefits and opportunities for children, it also presents significant challenges and risks. It becomes very important to discuss the cybercrimes which are growing day-by-day.\(^6\)

### 4. ONLINE CYBER CRIMES AGAINST CHILDREN

Cybercrime, the most recent and intricate form of criminal activity, involves the misuse of computers and the internet for various illicit purposes. These include cyber pornography, stalking, email bombs, viruses, and web jacking. Additionally, criminals exploit the internet for child abuse, posing a significant threat to young individuals. The advancement of technology has introduced new avenues for violence and harm in cyberspace, posing risks to children and adolescents.\(^7\) They are discussed below:

\(^5\) Ibid.

\(^6\) Dr. Dalbeer Lal, “Protecting the Child from the Evil Effects of the Digital Age” 10 International Journal of Creative Research Thoughts (IJCR T) e74 (2022).

1. **Cyberbullying**—Cyberbullying refers to the deliberate and persistent use of computers to harass, harm, embarrass, humiliate, or threaten someone else. Bullying using digital platforms, such as computers, tablets, and cell phones, is known as cyberbullying. Cyberbullying may happen via text messages and applications, as well as online in social media, forums, and video games where users can watch, interact with, and share material. It may involve disclosing sensitive or personal information about another individual, which might be embarrassing or degrading. Cyberbullying may often cross the line into illegal or criminal activity. It is one of the common cyber threats faced by children and young people. Though cyberbullying can impact anyone yet due to limited understanding of cyber threats, children become easy victims of cyberbullying. When students bully, they usually target people who are seen as weak, socially isolated, or who might not be aware of social standards. This can happen in person or through technology.

2. **Cyber Grooming**—it occurs when a person establishes an internet friendship with a young person and coerces or fools them into engaging in sexual activity. The cyber groomers can use gaming websites, social media, email, chat rooms, instant messages, etc. by creating a fake account and pretending to be a child or having the same interests as of the child.

3. **Child Pornography**—It is the representation of a young person in audio, video, or textual form partaking in actual or simulated explicit sexual behaviours using a variety of mediums, including digital, optical, and electronic. It entails using a minor for sexually suggestive activities. Another scenario is when a visual representation has been made, altered, or changed to suggest that a minor is having sex. It is nothing more than the sexual abuse and exploitation of minors by other children, which has a direct negative impact on the physical and mental health of the children involved.

4. **Online Gaming**—Concern over children playing video games has been raised in a variety of contexts; legislators, parents, and the media frequently highlight concerns about how children engage with games and their potential for addiction. UNICEF Innocent’s expert on digital technology and child rights, Kardefelt-Winther said. “As more and more children around the world play online games, society needs to learn more about how we can help our children balance the many positive aspects of online gaming with some of the riskier or potentially harmful aspects.” Because online gaming is one of the largest entertainment industries in the world, expanded internet capabilities, mobile technologies and affordable connected devices have opened the door to millions of gamers including large numbers of children.

5. **Online Sexual Harassment**—Unwelcome sexual advances, request or demand for sexual favour, and other verbal or physical conduct of a sexual nature. "Sexual harassment" encompasses both actions of a sexual character that an individual finds offensive or terrifying, as well as actions carried out with the clear intent to degrade the dignity of another person (i.e., purpose).

6. ** Sexting**—Self-production and posting of intimate pictures, sexually explicit conversations, posting / sharing of intimate pictures.

7. **Cyber Stalking**—Cyber-stalking is the term for stalking that takes place using information and communication technology in "cyberspace." A variety of platforms and online communities, such as

---

10 Ibid.
11 Ibid.
email, chat rooms, message boards, newsgroups, instant messaging, and keylogging, can be used by cyberstalkers. A variety of behaviours, such as threats, libel, defamation, sexual harassment, or other acts intended to subdue, persuade, or threaten their victim, may be involved.  

8. Camera Hacking - When malware that was downloaded with an attachment is used to snap pictures of people without their permission, this is known as camera hacking. These types of crimes can be committed with cell phones that do not have a security camera. Child sexual assault broadcast in real time. Child sexual assault is broadcast in real time to spectators who are located in faraway areas, a practice known as "live streaming."

9. Social Trolling - Social Trolling is posting inflammatory messages or visuals about a person or organisation in an online community with the express purpose of causing humiliation or nuisance to the object of trolling.

10. Profile Hacking - Profile Hacking happens when your email or social networking site is accessed by a probable stalker who then compromises it.

11. Picture Morphing People who post images on social networking sites can be taken advantage of by morphing one person's face to another's body and publicising it to frighten or blackmail the individual.

5. LEGISLATIONS ON CYBERCRIME IN INDIA

The child rights are enshrined in the constitution and protected through specific laws and regulations against cybercrime. In the Indian context, child rights are protected by various provisions in the Constitution of India, as well as specific legislation such as the Protection of Children from Sexual Offences (POCSO) Act, Information and Technology Act 2000 and Indian Penal Code, Data Protection Act 2021.

The Indian Constitution stipulates that certain laws and rules must be passed to safeguard children. Special laws for the protection of children must be provided by the state. India has a number of laws that address protecting children and their internet rights. Although India does not have a specific law to protect the rights of in this digital era, but being a signatory of the convention and after ratified it in year 1992, India is continuously making efforts to ensure the protection of children from all kinds of exploitation and to protect their rights. In this regard, India has enacted number of laws to save the rights of children in physical world as well as in cyber world. These laws are described as here under:-

A) Information and Technology Act 2000

One of the most important pieces of law that provide security for internet activity is the Information Technology Act of 2000. There are several provisions in this Act that address different types of cybercrimes. It sets fines for unauthorised access to data and computer harm brought on by malware, phishing, botnets, viruses, and other cyberattacks.

---

13 Supra note 3.
14 Ibid.
16 Ritu Chhabra and Dr. Sushil Kumar Singh, “Rights of Children in Cyber World: Indian Perspective” 43 Sambodhi 21 (2020).
Section 67B of this Act contains a dedicated provision aimed at safeguarding children on online platforms.

“Sec 67B: The punishment for publishing or transmitting material depicting children in sexually explicit acts or conduct in electronic form is outlined as follows:

1. Any individual who publishes, transmits, or causes to be published or transmitted material in any electronic form depicting children engaged in sexually explicit acts or conduct.
2. Those who create text or digital images, collect, seek, browse, download, advertise, promote, exchange, or distribute material in any electronic form depicting children in obscene, indecent, or sexually explicit manners.
3. Individuals who cultivate, entice, or induce children into online relationships for sexually explicit acts or in a manner that may offend a reasonable adult on computer resources.
4. Those who facilitate the online abuse of children.
5. Individuals who record in any electronic form their own abuse or that of others pertaining to sexually explicit acts with children.

Upon first conviction, offenders may face imprisonment for a term of up to five years and a fine of up to ten lakh rupees. In the event of a second or subsequent conviction, the punishment may include imprisonment for a term of up to seven years and a fine of up to ten lakh rupees.¹⁷

Section 66C explicitly addresses cybercrimes related to identity theft. It outlines penalties for individuals who knowingly and deceitfully use personal information, such as passwords or electronic signatures, belonging to others.¹⁸

Under Section 66E, capturing images of private body parts, disseminating, or transmitting them without the individual's consent is deemed punishable. Those convicted may face imprisonment for a maximum of three years and/or a fine of up to Rs 2 lakh.¹⁹

B) POCSO Act, 2012

The Protection of children from sexual offences Act, 2012 is a legislation enacted to protect children below 18 years of age from all forms of sexual offences including sexual assault, sexual abuse, sexual harassment, and child pornography.

Section 11²⁰ of the POCSO Act provides sexual harassment. A few instances involving electronic media are:

a. An individual displaying pornographic material to a child with sexual intent via any electronic medium would be deemed to have sexually harassed the child.

b. A person who constantly contacts a child through any electronic media is said to commit sexual harassment.

c. If a person threatens a child through any electronic form to use any body of the child or the child involved in a sexual act whether real or fabricated commits sexual harassment.

d. Allures a child for pornographic purposes.

Sexual harassment is punishable under Section 12²¹ of the POCSO Act. Any individual who commits the crime of sexual harassment faces a fine in in addition to up to three years in jail.

¹⁷ The Information Technology Act, 2000 (Act No. 21 of 2000), s. 67B
¹⁸ Id., s. 66 C
¹⁹ Id., s. 66 E
²⁰ The Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012), s. 11
²¹ Supra note 3, s. 12
Section 13 of the POCSO Act delineates the prohibition of using children for pornographic purposes under the law. It states that any individual who utilizes a child for their own sexual gratification through any electronic media, whether for personal use or distribution, is considered to have exploited the child for pornographic purposes. This encompasses the creation of obscene representations of the child, the display of the child's sexual organs, and the depiction of a child engaged in a sexual act.

Section 14 of the Act outlines penalties for using a child for pornographic purposes. Offenders under Section 13 face imprisonment for a minimum of five years along with a fine. Upon subsequent convictions, the minimum imprisonment increases to seven years, again accompanied by a fine. Additionally, if the individual involved also commits offenses under Section 3, Section 5, Section 7, or Section 9 by personally engaging in the pornographic acts, they will be subject to punishment under Section 4, Section 6, Section 8, or Section 10, respectively, in addition to the penalties outlined in Section 14.

Section 15 of the Act delineates penalties for storing pornographic material involving a child. Individuals found to be storing or possessing such material with the intent to transmit or distribute it without reporting it to the authorities will be subject to a fine of no less than Rs. 5,000 upon the first conviction, and no less than Rs. 10,000 for subsequent convictions. If the material is stored or possessed for transmission, display, or distribution in a manner not prescribed by law for reporting, the offender may face imprisonment for up to three years, a fine, or both. Those who store or possess the material for commercial purposes may face imprisonment for a minimum of three years, extendable to five years, or a fine, or both. For subsequent convictions, the imprisonment may range from five to seven years, with the possibility of a fine or both.

According to Section 16 of the Act, aiding and abetting the commission of any of the aforementioned acts is illegal.

C) Indian Penal Code

The Indian Penal Code (IPC) encompasses various offenses, including those committed online such as criminal intimidation, hate speech, and defamation.

Section 153 A of the IPC addresses hate speech, defining it as any act promoting enmity between different groups based on various grounds, detrimental to societal harmony.

Section 419 tackles cheating by impersonation, stipulating imprisonment for up to three years, a fine, or both for offenders.

Section 354D pertains specifically to stalking women, carrying penalties of imprisonment for up to three years with a fine for the first conviction and up to five years with a fine for subsequent convictions. Defamation, covered under Section 500, includes cyber stalking and carries punishments of up to two years of simple imprisonment, a fine, or both.

Criminal intimidation, outlined in Section 506, can lead to imprisonment for up to two years, a fine, or both.

---

22 Id., s. 13
23 Id., s. 14
24 Id., s. 15
25 Id., s. 16
26 The Indian Penal Code (Act No. 45 of 1860), s. 153 A
27 Id., s. 419
28 Id., s. 345D
29 Id., s. 500
30 Id., s. 506
Section 292\textsuperscript{31} prohibits the possession, sale, etc., of obscene material. Although the IPC doesn't specifically address offenses against children, these provisions can be applied in such cases.

**D) National Cyber Security Policy -2013**

The Indian government implemented national cyber security with a number of goals in mind. The prevention and appropriate investigation of cybercrimes, especially those against minors, is one of the policy's goals. It offers a suitable legislative framework to improve the capabilities of enforcement. Its goal is to raise public awareness about cyber security. The measure also safeguards citizens' data, forbids invasions of their privacy, and shields them from financial damages brought on by cybercrimes such data thefts that result from invasions of privacy.

**E) The Digital Personal Data Protection Act, 2023**

The Act provides a number of protections to ensure that children's privacy is maintained. The clause stating that consent must be given by the age of 18 is among the most significant. The Act stipulates that a data fiduciary must get permission from the guardians before processing a child's personal data. It also suggests requiring mandatory registration with the data protection authorities for data fiduciaries that deal only with minors. Processing children's data and offering them services is seen as a qualifying criterion for identifying a significant data fiduciary. Significant data fiduciaries are subject to extra requirements outlined in the legislation. It is against the law for data fiduciaries to follow or monitor children's data or handle personal information in a way that might endanger children.

**Lacunae in Indian laws**

Despite the fact that many crimes against children are illegal in India, some acts are not recognised as crimes. In India, cyberbullying, which is illegal in many other nations, is nonetheless a serious crime. Sexting works in the same way. Because there is no legal mechanism in Indian law for the punishment of cyberbullying and sexting, these acts are not regarded as significant crimes there. The act of trafficking children with the aim to use them for sexual exploitation is illegal, but the act of trafficking children with the goal to create pornographic or obscene content is not specifically covered by the law. It also says nothing about cybergrooming, which is another crime committed against children in our nation at an alarming rate that might ultimately lead to their death. Cybergrooming is done with the intention of sexual exploitation.

Both the IT Act of 2000 and the POCSO Act of 2012 need to be amended.

A. A amendment to the POCSO Act of 2012 that makes it illegal to promote or counsel sexual activity with someone under the age of 18 in any written document, graphic depiction, audio recording, or portrayal.

B. In connection with this, the IT Act, 2000 was amended to provide for punitive measures against individuals who give minors access to pornography and against those who obtain, create, or disseminate information on child sexual abuse.

C. Accountability of agencies receiving actionable intelligence: This would allow local police departments and law enforcement agencies across international borders to share intelligence in order to guarantee investigations.

\textsuperscript{31} \textit{Id.}, s. 292
D. Speedy legal deterrence through investigation and disposal: The required deterrence would be provided by expedited investigation and case disposal in addition to a thorough definition of child pornography and the modifications to the POCSO and IT Act.\textsuperscript{32} Since cybercrimes against children have increased so much, special attention needs to be given to this growing menace. Speedy trials and subsequent prosecutions could be a deterrent for current and future offenders. Consequently, not all facets of children's internet safety are covered under Indian legislation. This is still an area that requires development and law, as well as comprehensive protections for children's online interests.\textsuperscript{33}

6. JUDICIAL APPROACH

The Indian government has passed several laws to safeguard children's rights both offline and online. Unfortunately, we lack child-specific legislation similar to that of the United States, and the regulations that do exist are insufficient to protect children's online privacy rights. To safeguard children's rights and privacy in this digital age, the Indian judiciary interprets cyber laws and establishes recommendations in this respect.

In the case of Jayesh S. Thakkar v. State of Maharashtra, In response to the petitioners' letter about the abundance and accessibility of pornographic websites on the internet, the Chief Justice of the Bombay High Court considered the letter to be a writ petition. The division bench issued an order establishing a committee to provide ideas and proposals for stopping it, managing it, and safeguarding minors' access to pornographic websites and other offensive content on the internet.\textsuperscript{34}

The Airforce Bal Bharti School case, a 16 years old student had created a pornographic website to take revenge as he was teased for his pockmarked face. On one pornographic website, he posted photos of his professors and classmates that had been scanned and altered. The youngster was prosecuted under the Indecent Representation or Women Act, section 292, 293, and 294 of the IPC, and section 67 of the Information Technology Act, 2000. Nonetheless, the Juvenile Court granted the child bail.\textsuperscript{35} Further, in another case, in Mumbai, a Swiss Couple\textsuperscript{36} has gathered some children from slum area and then clicked their nude photographs forcefully. Later they uploaded these photos on website. The Mumbai Police arrested them for the offence of cyber pornography under Section 67 of I.T. Act and under section 292 and 509 of IPC.

Child pornography was not a factor in the Aneesh v. State of Kerala, 2023 case that the Kerala High Court determined. While the Kerala High Court and the Supreme Court of India have concluded that viewing adult pornography in private is not illegal under Section 292 of the IPC, downloading sexually explicit content that is intended for children is unquestionably illegal under the IT Act.\textsuperscript{37} A complaint was filed against the activist Rehana Fatima for uploading a video showing his children, who are between the ages of 8 and 14, panting in his pants under various provisions of the Juvenile Justice

\textsuperscript{32} Ritu Chhabra and Dr. Sushil Kumar Singh, “Rights of Children in Cyber World: Indian Perspective” 43 Sambodhi 21 (2020).
\textsuperscript{33} Ibid.
\textsuperscript{34} Ritu Chhabra and Dr. Sushil Kumar Singh, “Rights of Children in Cyber World: Indian Perspective” 43 Sambodhi 21 (2020).
\textsuperscript{35} Id, p. 26.
\textsuperscript{36} Ibid.
(protection) Act, POCSO Act, and IT Act. The Kerala High Court denied her request for bail, dismissing her argument that she was teaching her kids about sex education. In S. Harish v. Inspector of Police, the Madras High Court recently declared that downloading child pornography was not illegal under Section 67B of the Information Technology (IT) Act, 2000, quashing the legal proceedings.

7. CONCLUSION
The burgeoning growth of cyber crime poses a significant threat to children who are increasingly exposed to the internet. Despite the myriad benefits it offers, the digital realm also harbors numerous risks. Cyber criminals exploit vulnerabilities in online platforms to perpetrate various forms of harm against children, including cyberbullying, grooming, sextortion, and online exploitation. While legislations such as the Information Technology Act, POCSO Act, and Indian Penal Code aim to address cyber crimes, there remains a glaring gap in the legal framework concerning the specific protection of children in cyberspace. In the lack of specific legislation, children's rights to internet safety and privacy are compromised and they become more susceptible to abuse. Addressing this pressing issue requires concerted efforts from policymakers, law enforcement agencies, educators, and civil society organizations. There is an urgent need to enact comprehensive legislation that specifically targets cyber crimes against children, providing clear guidelines and stringent penalties for perpetrators. By bridging the gap between legislation, enforcement, and awareness, we can create a safer digital environment for children, ensuring that they can benefit from the vast opportunities of the internet without falling prey to its darker aspects. Protecting our children from cyber crime is not just a legal imperative but a moral obligation that requires collective action and commitment from all stakeholders.