



Legal Safeguards Against Child Cyber Abuse in India: A Critical Analysis and Reform Proposals

Shruti Chaurasia, Dr. Moumita Sen Chakraborty

LL.M. Student, Associate Professor and Associate Dean

School of Law, Galgotias University Greater Noida, India

Abstract: This paper focuses on a comprehensive analysis of the legal frameworks regarding the protection of children from cyber abuse in India. Key findings demonstrate a significantly high frequency of cyber abuse, including cyberbullying, harassment, grooming, and exposure to inappropriate material. The research identifies the laxity of regulations and the nature of the internet as key factors contributing to these abuses. The book examines the principal factors that increase children's susceptibility to such abuses. This study also analyses the legislative actions in India pertaining to the cyber exploitation of minors. He critically assesses the sufficiency of certain legislation, such as The Information Technology Act of 2000 and the Protection of Children from Sexual Offences Act of 2012, in light of the proactive measures taken to address the evolving nature of cyber threats. This research identifies deficiencies in enforcement, understanding, and execution about technology's role in ensuring children's welfare and safety in the expanding digital landscape.

Keywords: Children online abuse, the digital world, online exploitation, exposure to dangerous content, online harassment, POCSO Act, and regulation.

Introduction:

In the cybernetic age children are facing unprecedented risks can be subjected to vicious cyber exploitation that has sparked the attention of policymaker around the world. "However, it needs adequate attention in form of research and scrutiny especially in the context of India as it focuses on understanding the cyber abuse maze that Indian children face."¹ It examines its different manifestations and their implications. This study aims to address the deficiencies in current legal frameworks, laws, policies, and mechanisms related to safeguarding children from violence in the digital realm, highlighting the importance of awareness regarding this pervasive

¹ Janna Anderson & Lee Raine, The Positives of Digital Life, PEW RESEARCH CENTER.

issue.”

Recent developments in satellite television, such as Jammu and Kashmir emerging as one of India's latest frontline bachelor states populated by young families, have significantly contributed to the transition towards internet-enabled services. The experience of residing in a rapidly expanding population presents a dual challenge, as the increased accessibility of the internet, along with interconnectivity and migration, creates opportunities for the exploitation of children and contributes to the alarming rise of international networks. The various facets of internet accessibility give rise to issues such as cyberbullying, grooming, and the desexualized exploitation of online religious content.

Understanding Legal Definitions of Minor and Abuse Against Minors:

The definition of "minor" in Indian law varies according to the context and intent of particular statutes. Any person below the age of eighteen is considered a child under the “Protection of Children from Sexual Offences (POCSO) Act” 2012. “The Juvenile Justice (Care and Protection of Children) Act” 2015, also explain minor as an individual who has not yet reached the age of eighteen, continuously maintains this age standard. However, a gender-specific distinction is made by the “Prohibition of Child Marriage Act” 2006, which forbids early marriage by classifying a male under 21 and a female under 18 as minors.

According to the “World Health Organization” (WHO), child abuse encompasses a wide variety of detrimental actions directed against youngsters. These include neglect, sexual exploitation, physical and psychological abuse, and the commercial use of minors. Such behaviours, whether active or passive, endanger the child's general development, health, dignity, and well-being. In order to guarantee that every child or teenager is raised in a secure and encouraging environment, these definitions emphasize the critical necessity for coordinated preventive measures.

Research problem:

Child cyber abuse is pervasive and severe in India, posing serious threats to children's safety and wellbeing in this Internet era. “In spite of current legal mechanisms and action, loopholes continue to exist in effectively countering this multilayered phenomenon.”² The insufficient reporting of child internet abuse instances, guardians' and caretakers' lack of knowledge about online dangers, the changing strategies used by abusers to take advantage of children online, and the necessity of updating laws frequently to handle new threats are the main issues. The lack of comprehensive information about the type and prevalence of child internet abuse in India makes it more difficult to informed decision-making and customized interventions. These issues must be resolved by a contextual comprehension of the intricate aspects associated with child cyber abuse, followed by practical solutions to enhance legal protection, capacity building, awareness campaigns, and operational mechanisms. This project aims to address critical concerns in order to illuminate the pathway to a secure online environment for children. Presently, India's legislation and regulations are insufficient in protecting children from the escalating threats of internet exploitation. This creates substantial deficiencies in prevention,

² available at <https://wcd.nic.in/act/pc-so-act-2012>.

identification, and prosecution, thereby exposing millions of children to risks. A study and modification of existing laws and practices is necessary to enhance the safety and rights of children on the internet.

Research Objectives:

The purpose of this study is to examine the frequency and features of child cyber abuse in India, to evaluate how well the current legal system, institutional mechanisms, and policies protect kids from the dangers of the internet.

to examine and assess the laws and regulations already in place in India that protect kids from being exploited online.

to determine the shortcomings and difficulties in putting the laws and policies into practice, to assess how important organizations, such as legislators, law enforcement, and internet service providers, contribute to the fight against child exploitation on the internet. suggest workable legislative and policy changes to improve kid safety in India's internet environment, based on precedents from other countries.

Research Hypothesis:

In order to improve the protection of children from online abuse, it was anticipated that there would be noticeable lack in the implementation and application of current legislative structure, which would need to be addressed by specific interventions. "The imperative for specific legal structure that guarantees all round safeguarding of children online is strongly felt as India's legislation, in keeping pace with evolving forms of online child abuse, thus creating huge policy lacunae as a drag in the effective functioning of prevention, detection, and enforcement activities."³

Research scope:

With an emphasis on prevalent forms such as digital assault, internet bullying, and being exploited, the present research investigates child cyber abuse in India. In addressing these concerns, the study will critically assess the effectiveness and sufficiency of current legal frameworks, with a focus on the sexual offences (POCSO) Act of 2012 and the Information Technology Act of 2000. In order to increase protections and awareness, it will look at how laws relevant to child internet abuse are enforced and suggest measures for academics.

Research Question:

1. Prevalent cyber abuse categories for minors in India?
2. How well do Indian laws and practices protect minors from digital abuse.?
3. What are the biggest obstacles to state child online abuse enforcement?
4. What can be done to raise awareness and safeguard Indian children from internet abuse?

³ A. Chawla & A. Garg, *Cyber Safety for Children: A Study of Awareness Levels Among Parents and Guardians in India*, 6 Int'l J. Eng'g & Computer Sci. 21907, 21907-12 (2017).

5. How law enforcement and internet service providers affect legal protections for Indian children against online exploitation. enforcement problems.

Understanding the child exploitation in India:

Confronting the Issue of Child Exploitation on the Internet The ubiquity of the internet has resulted in vulnerable children being exposed to a variety of online dangers, which has consequently led to the emergence of a significant problem in India: the exploitation of children through cyberspace. The following are examples of some of the most serious dangers: child pornography, cyberbullying, online grooming, and trafficking. As a result of the presence of predators waiting in the wings, social media platforms, games, and other messaging applications are all exploiting minors for the purpose of achieving their unlawful and profitable goals. In addition to the Prevention of Children from Sexual Offenses Act (POCSO) and the Information Technology Act, there is a lack of appropriate digital literacy among children and, in particular, among parents. There are efforts being made by the government, in conjunction with groups from civil society, to enhance channels for reporting and raising awareness. Coordination between schools, parents, law enforcement, and technology companies is necessary in order to make the internet a safer place for children and to prevent them from being exploited online. This is necessary in order to ensure that the internet is safer. Different types of online exploitation are defined as follows: Exploitation of children for the purpose of using the internet to abuse or exploit children is a dangerous activity that is known as online exploitation of children. The act of persuading children to transmit inappropriate photographs or videos, grooming them on the internet by earning their trust in order to later exploit them, and cyberbullying or other forms of harassment or threats conveyed via the internet are all examples of this. It also addresses concerns such as the forced labour of children, the trafficking of children, and the exposure of children to content that is unsuitable. It is possible that all of these things are on social networking websites, game applications, and messaging apps, and the children are unaware of the full significance of these particular actions. It will be necessary to raise awareness and implement strong security standards in order to protect children online.

Impact on Children:

The effects of online child abuse on a child's development can be devastating and chronic. Exposure to harmful content or abusive behaviour on the internet can cause emotional and psychological discomfort in children. They feel ashamed or guilty, nervous, depressed, and afraid. When kids feel intimidated when interacting with others online, it can lead to trust issues in their real and online social lives. "That impacts their academic progress and their interpersonal relationships. Trauma also results in psychological issues such as low confidence and, in severe cases, self-injury. Children end up being reclusive or withdrawn, losing confidence to play outside. These are experiences that can be prevented in the early stages by intervention, guidance from parents, schools, and professionals."⁴

⁴ S. Sharma & M. Pandit, *Child Online Protection: Issues and Challenges*, 14 Int'l J. Hum. Rts. Healthcare 258, 258-71 (2021).

Types of Indian Child Cyber Abuse:

The previous section will thoroughly look at the many forms of cybercrime that Indian youth encounter. This will explain the frequency, seriousness, and effects of child abuse, intimidation, stalking, and getting exposed to harmful web pages using actual case studies and examples. The negative impacts of cybercrime on children's social interactions, performance in school, psychological wellness, and confidence will be discussed in this section.

India's Legal Mechanisms for Safeguarding Children in the Digital Environment:

The legal framework in India designed to shield kids from online abuse is critically examined in this study. Important laws include the "Juvenile Justice (Care and Protection of Children) Act" 2015, which protects children's safety and welfare, including those who are victims of online exploitation, and the "Information Technology Act", 2000, which deals with cybercrimes and the dissemination of content involving child sexual abuse. To improve children's digital safety, regulatory organizations such as the National Commission for Protection of Child Rights (NCPCR) have released guidelines in addition to law regulations. Although these rules provide a basic framework, the quick development of technology necessitates frequent revisions, efficient enforcement, and raised public awareness to guarantee children's complete protection in the online world.

This section highlights issues and gaps in the legal system for protecting children from cyber abuse:

Despite the laws that are currently in effect. We'll talk about issues like legal challenges, data acquiring challenges, and the need for better law enforcement-online service coordination. The section will also cover the challenges guardians and teachers have when instructing kids on online safety and how to handle instances of online bullying.

The following are some of the reasons why India needs its government to pass comprehensive legislation:

The fast expanding issue of child abuse in the digital sphere cannot be adequately addressed by India's current legal system. Despite the existence of certain statutory requirements, there are still large gaps in their precision, consistency, and enforcement. The lack of a consistent definition of "child" across different laws is a serious issue since it makes legal procedures more difficult and compromises protections. Legislation specifically addressing cyberbullying and other child-specific online offenses is also desperately needed. Digital service providers and social media sites who disregard child protection laws must also face severe penalties.

India's legal framework for combating cybercrimes is the Information Technology Act of 2000.

Section 66B: This provision identifies possible unlawful computer or communication hardware procurement and specifies a three-year prison sentence as the penalty. Given the seriousness of the offense, a punishment of up to Rs. 1 lakh may also be imposed. Digital signatures, password hacking, and other forms of identity theft are the main topics covered under

Section 66C: The maximum penalty under Section 66C is 3 years imprisonment and a 1 lakh rupees.

Section 66D: This section discusses using computer resources to impersonate someone else in order to cheat. If found guilty, the maximum penalty is three years in prison and the maximum punishment is one lakh rupees. Addresses used without the owner's consent also violate.

Section 66E: which prohibits sending pictures of people.

Section 67 B: This significant piece of legislation provides protection for online activity. This statute covers offenses against children that occur online.

The law considers the aforementioned parts to be crimes against children. content on any electronic platform that depicts minors engaging in sexual activity, pornography involving children, or hazardous content.

Bhartiya Nyaya Sanhita (2023): Law enforcement organizations may consult the following parts if the IT Act is found to be inadequate in the fight against cybercrimes.

Section 294: Initially put into place to stop the sale of pornographic goods, it has now expanded to cover a wide range of cybercrimes, such as the electronic distribution of pornographic or sexually explicit content involving children.

Section 77: Without a woman's consent, it is illegal to record or share her intimate body parts or behaviours.

Section 78: It defines and addresses stalking, including offline and online forms of cyberstalking, which is defined as the persistent use of technology to pursue a woman.

The POCSO Act of 2012 delineates sexual harassment:

Section 11: It encompasses any individual who persistently engages with a child through internet communication or issues threats regarding the child's physical autonomy or seeks to involve the child in venereal activities regardless of threats are tangible or merely perceived this constitutes sexual intimidation.

“The (POCSO) Act's Section 13 defines the legal ban on exploiting children for pornographic purposes. Section 14 of the Act explains the effect of engaging a child in an pornographic role.”⁵

Data Protection Bill 2021:

There are several legislative safeguards in place to protect children's privacy. One of the most crucial is that before processing a child's personal information, the data custodian must get the guardians' approval. Furthermore, it advises data guardians who have direct contact with minors to register with the appropriate data security authorities. Data guardians are prohibited from doing anything that would endanger children, such as improperly monitoring, surveilling, or manipulating their data. The main objective of this measure, which would amend the two acts following a report by an integrated parliament committee, is to protect children's internet privacy. Cybercrime, data security, deepfakes, platform competition, online security, and the adverse impacts of artificial intelligence are all included in the Digital India 2023 bill. In

⁵ The Protection of Children from Sexual Offences Act, 2012.

order to provide comprehensive regulation of India's digital sphere, this new bill seeks to address a number of issues, including cybercrime, data protection, deep fakes, network competition, safety on the internet, and the detrimental effects of AI. Law changes to stop cyberbullying: It wasn't until 2013 that the Indian Penal Code, 1860, specifically addressed online harassment and crimes against women. Section 354A was introduced to Section 354D of the IT Act Amendment 2000 by the Criminal Amendment Act of 2013 in order to modernize the Indian Penal Code of 1860.

The function of internet service providers and law enforcement:

Lack of Technical Expertise: The majority of Indian law enforcement organizations are not equipped with the technology know-how required to properly monitor, look into, and prosecute cases of child exploitation that occur online.

The majority of authorities lack the specific tools and training required to tackle cybercrimes, particularly those employing the dark web, encryption, and anonymous browsing.

Jurisdictional Issues: Due to the worldwide nature of the internet, internet-based exploitation frequently transcends national boundaries, making it challenging for local law enforcement to handle such instances.

The lack of defined structures for international collaboration makes enforcement easier. Limited Resources: Many Indian law enforcement agencies are under-resourced as a result of the rise in cybercrimes. Lack of personnel and the newest investigative tools make it difficult to respond to allegations of child exploitation online in a timely and effective manner.

Internet Service Providers (ISPs):

Insufficient information Filtering: ISPs frequently possess inadequate mechanisms to obstruct offensive content, particularly child sexual abuse material (CSAM). Some ISPs actively work to restrict illicit content, while others either decline to invest in such technologies or lack the necessary technical infrastructure.

Encrypted and Security of Data:

As the use of encrypted communications becomes more widespread, it becomes more difficult for Internet service providers (ISPs) to identify or intercept actions that are related to the potentially harmful exploitation of children. "This has come to be a serious issue since encryption systems protect consumers' privacy while at the same time complicating the capture of criminals. Policy gaps and issues: The lack of an extensive, specialized body of law that specifically deals with the diverse and evolving nature of online child abuse, including cyberbullying, grooming, and the dissemination of child sexual abuse material (CSAM), is a policy gap that hinders India from effectively safeguarding children from exploitation on the Internet."⁶ Although specific elements of cyber exploitation are restricted by laws like the Protection of Children from Sexual Offences (POCSO) Act and the Information Technology (IT) Act, these restrictions were not designed to comprehensively address the distinct issues presented by the digital realm.

⁶ Dr. Dasgupta M., Cyber Crime in India A Comparative Study: Eastern Law House, New Delhi, Page no.8-9

Internet Anonymity:

It is difficult for law enforcement agents to detect, track, and apprehend criminals who are using the internet because of the anonymity that the internet provides. The worldwide nature of the internet, along with the anonymity it provides, makes it more difficult to implement laws that are already in place and to address concerns of jurisdiction.

Insufficient Digital Literacy:

Parents, children, and law enforcement personnel are inadequately informed about the dangers of online exploitation and the preventive strategies accessible to them. Insufficient digital literacy results in both the underreporting of occurrences and inadequate oversight of children's online activity. Insufficient Digital Literacy: Parents, children, and law enforcement personnel are inadequately informed about the dangers of internet exploitation and the methods to avert it. The underreporting of occurrences and inadequate monitoring of children's online activities result from insufficient digital literacy levels. Insufficient Law Enforcement Training: The majority of law enforcement agencies lack the technical proficiency and specific training necessary to address cybercrimes against children. This complicates the thorough investigation and prosecution of online abuse cases, especially when advanced methods like encryption or sophisticated anonymization technologies are employed.

The process of implementation:

India has established stringent laws against child exploitation, such as the POCSO Act and the Information Technology Act, which facilitate the protection of children from harmful online activities. An implementation gap persists. These children and their parents exhibit lower levels of digital literacy. "This is too much harder to identify these dangers and report them. Increasingly, tracking and arresting the perpetrators in the cyber world becomes difficult for the law enforcement because of the anonymity of the internet. Most of the time, there are under equipped units like cybercrimes units like cybercrime units which are either equipped with latest gadgets nor trained enough to handle all the crimes being committed online with children. The reporting systems are mostly inaccessible or inconvenient, hence becoming difficult for the victims to come forward."⁷ Thirdly, the absence of skilled personnel to undertake child-sensitive investigations and judicial proceedings results in delays in the administration of justice. The awareness and coordination of stakeholders, including social media, law enforcement agencies, and government ministries, are still evolving. The absence of cooperation may undermine the efficacy of these regulations intended to protect minors from internet exploitation. Increased efforts must be focused on the more effective implementation of existing legislation.

Awareness:

The swift proliferation of internet access and mobile phone usage presents both opportunities and risks for youngsters in India, particularly for education, entertainment, and social interactions. This necessitates advocating for heightened understanding regarding internet child safety. Alternative public and governmental

⁷ Dr. Ahmad Farooq, Cyber Law in India (Law on Internet): New Era Law Publication, Faridabad.

initiative. “The Cyber Swachhta Kendra promotes guidelines for safe and better use of internet. Digital literacy programs in schools have also been encouraged, which provide students with required information on cybersecurity as well as ethical conduct in online operations.”⁸ To help people stay safe when using the internet, non-governmental organizations (NGOs) and advocacy groups like Cyber Peace Foundation and Save the Children run awareness campaigns.

Suggestions and Best Practices:

This section will offer suggestions for improving child protection from cyber abuse in India based on an analysis of the literature and the law currently in effect. Better legal revisions, the establishment of specialized cybercrime units, better instruction in digital literacy in schools, and cooperation between law enforcement, schools, parents, and internet service providers are some possible ideas.

The Function of Technology in Safeguarding Children Technological Solutions: Technology will primarily protect the child from online dangers when they obtain access to the internet at various stages of life, whether for educational or recreational purposes, among others. Parental solutions that include effective parental control software, content filtering mechanisms, and monitoring applications are essential to ensure a safe internet experience for children. The applications establish parameters for inappropriate content, monitor children's actions, and obstruct objectionable material. Gaming applications and social media platforms incorporate inherent safety safeguards, including age verification systems that facilitate the reporting of inappropriate conduct.

A distinct statute delineating offenses against minors in the digital realm is preferred for addressing this issue. Digital exploitation, encompassing online child offenses, must be recognized and considered in the adjudication of the case. This legislation must govern virtual platforms while establishing explicit boundaries of accountability among the various stakeholders, including technology companies, parents, and educators, and delineating clear standards for addressing digital exploitation. An effective statute should protect children's rights to privacy and autonomy while enforcing stringent penalties on offenders. The primary necessity for the government to achieve proactive and effective child protection in cyberspace is a highly specialized legislative framework that can evolve with technological advancements. “Cooperation internationally will be included in it in light of international cooperation to combat such offenses as child exploitation and abuse over the internet, it will complement knowledge and capacity building in enforcement, thus strengthening protection for children.”⁹

Conclusion:

there has to be rapid, multi-stakeholder action to address the serious threat of child cyber abuse to the well-being of children in India. The present research has highlighted the most common forms of abuse, gaps in the

⁸ Cheng, L., Hu, X., Matulewska, A., & Wagner, A., Exploring cyberbullying: A socio-semiotic perspective, International Journal of Legal Discourse, 5(2), 359–378, (2020).

⁹ NCPCR, Preventing bullying and cyberbullying guidelines for schools
https://ncpcr.gov.in/uploads/1702548255657ad31ff39b4_preventing-bullying-and-cyberbullying-guidelines-forschools.

current legislation, and difficulties in enforcing it. An effective reaction must include reforming the law, improving stakeholder collaboration, and intervening. The rapid evolution of cyber risks necessitates the continual review and revision of existing laws to account for emerging forms of exploitation and technology. To strengthen investigation ability and allow for prompt intervention, it will be necessary to implement capacity-building programs for the law enforcement agencies and to have effective public-private partnerships. Strict penalties and centralized reporting systems, such as national hotlines, can serve as effective deterrents.

Finally, India needs to bring its child protection policies in line with international best practices. A specific, comprehensive law on online child exploitation needs to be enacted. With awareness, proactive enforcement, and responsive policy frameworks, India can make its digital space a safer place for its most vulnerable citizens—its children.

References:

1. *Research India Publications*, Definition of Cybercrime,
2. *Oxford English Dictionary*, Definition of Cybercrime,
3. Naavi, Cyber Crime Definitions in India,
4. *Cybercrime.org.za*, Definition of Cybercrime,
5. J.W.C. Turner, *Kenny's Outlines of Criminal Law* 17 (19th ed. Cambridge Univ. Press 1966), cited in Talat Fatima, *Cyber Crime* 64–68.
6. R.C. Nigam, *Law of Crimes in India: Principles of Criminal Law* vol. 1, at 6 (Asia Publ'g House 1965).
7. Talat Fatima, *Cyber Crime* 64–68 (1st ed. E. Book Co. 2011).
8. The Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).
9. Rahul, Research Note on Online Child Pornography Law in India (on file with author).
10. Nidhi Marothiya, Shraddha Kapoor & Vinita Bhargava, *Child Protection in India: Issues and Policies*, Dep't of Hum. Dev. & Childhood Studies, Lady Irwin Coll., Univ. of Delhi (India).
11. Dr. Dakshina Saraswathy, *Challenges in Child Rights and Child Protection in India*, Assoc. Professor, Kerala Law Acad., Thiruvananthapuram.
12. Nicole Rangel Menezes, *Child Protection in India* (unpublished manuscript) (on file with author).
13. UKCCIS Evidence Group, *Children's Online Activities, Risks and Safety: A Literature Review*, Int'l J. for Multidisciplinary Res. (IJFMR).
14. *Cyber Law Indian & International Perspective* By Aparna Viswanathan.
15. *Cyber Law Indian & International Perspective* By Aparna Viswanathan.
16. *A Practical approach to Cyber Laws* - by Mani.
17. *Network Security: A Hacker's Perspective* By Ankit Fadia.
18. *Cyber Laws* By Dr. Gupta & Agrawal.