UNVEILING THE GAPS IN CHILD PROTECTION LAWS AMIDST ONLINE SEXUAL ABUSE IN INDIA

Ananya Malhotra, Christ Deemed to be University, Bangalore

ABSTRACT

In the contemporary context, information technology has been seamlessly integrated into the structure of everyday existence, catering not only to adults but also engaging children as young as four or five years old. Amid this captivating digital landscape, however, there is a huge amount of inappropriate and uncensored content on the Internet. Furthermore, there is a disturbing presence of criminals who deliberately target vulnerable children, to exploit and harm them. These criminals commit serious crimes such as child pornography, sexual harassment, and cyberbullying. A large study conducted by India's Ministry of Women's and Child Welfare in 2007 examined more than 12,000 children and amazingly revealed that 4.4% of them had had a terrible experience with child pornography.

This study focused on assessing the extent to which Indian law protects children from online sexual abuse, which is of primary concern. The main laws mentioned are the Information Technology Act 2000 and the Child Protection from Sex Crimes Act 2012. However, these laws have notable shortcomings. For example, Section 67B of the Information Technology Act regarding child pornography does not provide a clear definition of the term itself. Similarly, the Child Sex Crimes Protection Act 2012, while important, does not adequately address emerging cybercrime such as the use of stolen identities to exploit children online.

This study critically examines these gaps in the current regulatory framework in India, analyzing in depth their impact on the protection of children from online sexual abuse. The study offers a way forward by advocating stronger regulatory measures to adapt to the rapidly changing digital landscape. This involves not only clarifying definitions but also expanding the regulatory framework to deal with new cyber threats that specifically target vulnerable young people. Through an in-depth exploration of case studies, comparisons with other legal systems, and the formulation of policy recommendations, this article aims to stimulate meaningful discussion about the important task of protecting citizens.

Research Questions

- How can the existing legal framework in India be harmonized and strengthened to comprehensively address online child protection issues, such as child pornography, grooming, cyberbullying, and sexual harassment?
- What steps can improve child protection enforcement in the digital era, addressing gaps in aftercare services and police units?
- How can India strengthen international cooperation to combat cross-border cybercrimes, aligning with global standards in child protection?

Research Objectives

- Evaluate India's legal framework for child protection in the digital age, focusing on child safety online.
- Assess the practical implementation of child protection laws and propose improvements, including aftercare services and specialized police units.
- Analyze legal gaps, and suggest measures to strengthen and harmonize laws for comprehensive online child protection.

I. *Introduction*

In today's digital age, a significant portion of our daily lives is spent on the internet. From using apps like Whatsapp and social platforms like Instagram to conducting business on sites like TradeIndia or Indiamart, we are all "netizens" in addition to being citizens. The number of smartphone users has been steadily increasing, reaching over a billion in 2012, and it is estimated to have grown to 1.75 billion by 2014. This digital shift has also affected children, with many of them actively using the internet for various purposes. For instance, 7 out of 10 children in India shop online, 76% have Facebook accounts, and 9 out of 10 own a mobile phone. While parents and educators encourage children to use the internet to access information and communicate, there is often a lack of awareness about the potential risks to their safety and security in the digital world.

The internet, specifically the World Wide Web, provides a fertile ground for cybercriminals who exploit its vast anonymity and employ technical tricks, such as using proxy servers for spoofing, to conceal their true identities. These criminals can operate individually or as part of organized groups, targeting vulnerable children and committing various serious offenses.

These crimes include cyberbullying, child pornography, child grooming, sexting, sexual harassment, defamation, and other morally reprehensible acts. The World Health Organization defines 'child sexual abuse' as engaging a child in sexual activities that the child does not fully comprehend, making them unable to give informed consent due to their lack of mental development or preparedness, or engaging in activities that violate the laws or societal norms and taboos.

In this context, the paper focuses on addressing the issue of online child sex abuse, which encompasses various offenses where a child is sexually abused by a cybercriminal, including child grooming and child pornography. These crimes can also involve additional offenses like defamation or identity theft. The paper highlights the need for effective legal measures to combat these offenses, emphasizing that existing laws should provide clear definitions, elements of the offense, scope, and penalties for first-time and repeat offenders. It also points out the alarming statistics related to crimes against children in India, including a significant increase in cases of kidnapping, abduction, abetment to suicide, and rape.

While the National Crime Records Bureau reports on various crimes against children, there is a lack of specific data regarding online child sex abuse under the Information Technology Act and the Protection of Children from Sexual Offences Act (POCSO). This gap underscores the need for a more comprehensive approach to child protection in the digital era, which includes evaluating the adequacy of existing laws and their enforcement. In this research paper, we assess whether Indian laws sufficiently address the multiple threats to children on the internet and whether the provisions in place are robust enough to safeguard children in the digital age.

II. *Child Pornography and Cyber Bullying*

The advent of the internet and digital technologies has ushered in an era where children are increasingly exposed to various online threats. This section of the document provides an in-depth analysis of the legal framework in India concerning child protection in the digital age, with a specific focus on child pornography, child grooming, and cyberbullying.

Child Pornography and Grooming

Prior to 2009, the Information Technology Act of 2000 did not contain provisions addressing offenses related to child pornography and grooming. This legal vacuum was addressed through the IT (Amendment) Act of 2008, which introduced Section 67B[1]. This section explicitly

[1] Section 67B IT Act, 2000

criminalized child pornography and child grooming, but it had limitations in its definitions. It stipulates that individuals who publish, transmit, create, collect, seek, download, advertise, promote, or distribute content depicting children engaged in sexually explicit acts in electronic form could be imprisoned for up to five years and fined up to 10 lakh rupees. However, this provision lacked a clear definition of "child pornography," which was a significant shortcoming.

Surprisingly, the Indian Penal Code lacked specific sections dedicated to child pornography. Although Section 293 addressed the sale of obscene objects to those under 21 years of age, it did not specifically target child pornography. The need for comprehensive legal coverage in this domain led to the introduction of the Protection of Children from Sexual Offences (POCSO) Act in 2012. Section 13 of the POCSO Act dealt with the use of children for pornographic purposes. This section was comprehensive in its coverage, encompassing various forms of media and including both personal and commercial use. Section 14 of POCSO prescribed punishments for the use of a child for pornographic purposes, including imprisonment for up to five years, with stricter punishments for those who directly participated in pornographic acts involving sexual assault.[2]

Despite these legal provisions, inconsistencies and overlaps exist, especially between the IT Act and the POCSO Act. For instance, child grooming is punishable with a term of imprisonment of up to three years under POCSO, whereas the IT Act prescribes punishment of up to five years of imprisonment and a fine of up to 10 lakhs. To create a more coherent legal framework, it is imperative to address these discrepancies. The inconsistencies also necessitate amendments that include individuals who cause a child to be used for pornographic purposes. To create a comprehensive legal framework, it is suggested that the definition of child pornography from the POCSO Act be applied to the IT Act, widening its application to encompass digital media.

Even in cases where a child doesn't face physical exploitation, they remain vulnerable to online abuse through the use of web cameras, video conferencing, and various communication applications. Social networks are sometimes infiltrated by malicious individuals who deploy tools like keyloggers, steganographic files, and worms. These tools can surreptitiously activate a child's web camera without their knowledge or consent. Children are sometimes lured into taking objectionable photos of themselves, which can then be obtained by these criminals

[2] Ministry of Women and Child Development, Government of India (2007) Study of Child Abuse, India 2007

through methods like SMS, email, or capturing direct screenshots. These activities not only jeopardize a child's privacy but also expose them to the risk of cyber harassment, defamation, kidnapping, and even more severe consequences[3]. Therefore, it is imperative to strengthen the penalties within existing laws pertaining to child pornography and eliminate any inconsistencies to enhance their deterrent effect on criminals.

- **Addressing Cyberbullying**

The term "cyberbullying" lacks a legal definition in Indian law. In simple terms, it refers to using threats or other forms of coercion to mentally harass someone over the Internet or through electronic communication. Cyberbullying becomes particularly concerning when it is directed at children, and in this context, it is termed "cyberbullying of a child." A survey conducted by Microsoft revealed that 53% of children between the ages of 8 and 17 in India have been victims of cyberbullying. These incidents mainly occur on social media platforms and online chat rooms, often leading to depression, low self-esteem, drug addiction, and, in severe cases, even suicide.

Although Section 66A of the IT Act could be applied to cyberbullying, it was deemed unconstitutional and was subsequently struck down by the Supreme Court[4]. The Indian Penal Code addresses criminal intimidation but does not specifically address child sex abuse acts. Given the gaps in the legal framework, it is imperative to introduce provisions that explicitly address child sex abuse, including cyberbullying. These provisions should address the unique nature of online harassment and its impact on children.

In accordance with the Protection of Children from Sexual Offences (POCSO) Act of 2012, Section 11 is in place to prevent sexual harassment of minors. Section 11(v) specifically addresses a scenario where a child could potentially fall victim to cyberbullying within the context of sexual abuse. According to this provision, an individual is considered to commit sexual harassment against a child if they, with sexual intent, make threats involving any form of media. This could encompass the use of real or fabricated depictions through electronic means, film, digital platforms, or any other medium, which involves any part of the child's body or depicts the child engaged in a sexual act. Section 12 outlines the associated penalties, which may include imprisonment for a maximum of three years along with a fine.[5]

[3] Dr. Srivastava, S. (2012), Pessimistic side of information and communication technology, cyberbullying and legislation laws Internet Journal of Advance in computer Science and Technology 1(1) pp. 14-20
[4] Shreya Singhal vs UOI
[5] Ministry of Women and Child Development, Government of India, POSCO Act 2012

An additional situation that should be included to comprehensively cover cyberbullying in cases of child sexual abuse is when an individual threatens a child to make themselves available for sexual gratification purposes and maintains persistent contact with the child through mobile or internet platforms. Section 11(iv) of the POCSO Act addresses the offense of cyberstalking. However, it does not explicitly encompass the crucial element of the threat being used to convert or merge with cyberbullying, creating a significant legal gap in the protection of children from digital sexual abuse.

In conclusion, the existing legal framework in India requires amendments and greater clarity to address child protection in the digital age comprehensively. Specifically, the areas of child pornography, child grooming, and cyberbullying need a more comprehensive and coherent legal framework to better protect children from online exploitation and harassment. The legislative changes discussed would contribute to creating a safer digital environment for India's children.

III. *Sexual Harassment: An Overlooked Menace*

A child may be sexually abused in many other ways apart from child grooming, cyber pornography, cyberbullying, or stalking. Some of the acts are covered in Section 11 of the POCSO Act, 2012. Section 12 of the POCSO Act, 2012 is reproduced here for easy reference:

(i) Utters any word or makes any sound, or makes any gesture, or exhibits any object or part of the body with the intention that such word or sound shall be heard, or such gesture or object or part of the body shall be seen by the child, or

(ii) Makes a child exhibit his body or any form of media for pornographic purposes

(iii) Shows any object to a child in any form or media for pornographic purposes or

(iv) Repeatedly or constantly follows watches or contacts a child directly or through electronic, digital, or any other means or

(v) Threatens to use, in any form of media, a real or fabricated depiction through electronic, film, digital, or any other mode, of any part of the body of a child or the involvement of the child in a sexual act or entices the child for pornographic purposes or gives gratification therefor.

(vi) Explanation -Any question which involves "sexual intent" shall be a question of fact."[6]

[6] Ministry of Women and Child Development, Government of India, POSCO Act 2012

Section 12 of the Protection of Children from Sexual Offences (POCSO) Act, 2012, is a pivotal component of child protection legislation in India. It addresses various forms of sexual harassment against children but reveals shortcomings when dealing with modern threats. The Act, while comprehensive in some respects, lacks provisions to address the invasion of a child's privacy through cyber means, such as keyloggers or webcam-trigger software that surreptitiously captures a child's images without their consent. This section specifically criminalizes actions such as compelling a child to exhibit their body for pornographic purposes, displaying explicit content to a child, incessantly following or monitoring a child, and employing threats related to child sexual abuse for personal gratification. These provisions are indeed crucial in addressing certain forms of child sexual harassment, but they do not encompass the evolving challenges presented by digital technology.[7]

Furthermore, Section 66E of the Information Technology (IT) Act, 2000, pertains to the invasion of privacy in the digital realm. While it does offer a legal framework to prosecute offenders who infringe upon an individual's privacy, it falls short when the victim is a child. The existing legal provisions do not provide a sufficient deterrent for cybercriminals who engage in heinous acts of online sexual abuse against children. The relatively lenient penalties and limited scope of Section 66E fail to address the severity of these crimes.

To bridge these critical gaps in child protection laws, there is an urgent need to enhance the punishment for offenses related to online sexual abuse against children. Stricter penalties would not only serve as a more effective deterrent but also demonstrate a commitment to safeguarding the welfare and security of the most vulnerable members of society.[8] It is imperative to acknowledge the evolving nature of threats in the digital age and adapt the legal framework accordingly to ensure the comprehensive protection of children from online sexual harassment.

In the digital era, cyberstalking has emerged as a grave concern, where individuals harass others with various malicious intents. Often, this harassment is directed at enticing children into engaging in cyber pornography or acquiring their personal information for malicious purposes. India's legal framework has grappled with this issue.[9] Previously, Section 66A of the Information Technology (IT) Act, 2000, was intended to criminalize cyberstalking. However, it was criticized for its ambiguity and subsequently struck down. Although certain sections

[7] Medhashree Duta, TNN (2014,Jul 13) Under 13 kids social networking sites okay? The Times of India Article
[8] Julia Davidson, Internet Child Abuse, edited by Julia Davidson, Petter Gottschalk, chapter 1,pg 18.
[9] Seth Karnika, Protection of Children on Internet, Universal Law Publishing company, 2015. pg. 98

within the Indian Penal Code (IPC) do address related issues, they do not adequately encompass the severity of cyberstalking, particularly when it victimizes children.

To rectify the shortcomings within the existing legal framework, it is imperative to establish more stringent punishments for cyberstalking, particularly when children are the targets. Sections of the IPC, such as Section 509 (outraging the modesty of a woman), Section 506 (criminal intimidation), and Section 507 (criminal intimidation by anonymous communication), offer some legal recourse, but they fall short in providing a robust deterrent for cybercriminals. In light of the evolving digital landscape and its associated threats, there is a pressing need to establish a more comprehensive legal framework that can effectively protect children from online sexual harassment.

Child trafficking for sexual exploitation is a pervasive problem in India, affecting many children from a very young age. Immoral trafficking, once limited to physical spaces, has now extended its reach into virtual realms. Criminals have begun to misuse technology, including webcams, Voice over Internet Protocol, and videoconference applications, to record and disseminate child pornography or engage in illicit activities such as the sale and purchase of children for prostitution.[10]

While the IT Act addresses the issue of child pornography, it fails to provide clear definitions regarding the liability of intermediaries, such as app providers and website operators, who may inadvertently or knowingly facilitate online child abuse. Section 79 of the IT Act does offer some exemptions to intermediaries in certain cases, but the law requires further clarification. This is essential to ensure that intermediaries are held accountable for their roles in enabling child abuse online, whether directly or indirectly.

In Conclusion , Safeguarding children from online sexual abuse and harassment is an urgent and critical concern in today's digital age. While the existing legal framework in India reflects well-intentioned efforts, it reveals significant gaps that must be addressed promptly. To meet the evolving challenges presented by the digital landscape, the law needs to adapt and evolve accordingly. This adaptation should encompass newer forms of abuse, introduce stricter penalties for offenders, and ensure that intermediaries bear their share of accountability. By doing so, we can establish a safer environment for India's children, one that is resilient against the ever-changing nature of online threats. Protecting our children from online sexual

[10] Sen, S. (2005), Trafficking in Women &Children in India, New Delhi, India: NHRC.

exploitation is a moral imperative and a societal responsibility that necessitates a legal framework that is both robust and adaptable.

IV. *Lacunae in Implementation of Existing Law and Recommendations*

India, as a signatory to the Convention on the Rights of the Child, has enacted several laws to safeguard children from sexual abuse, including online exploitation. However, a closer examination reveals significant inadequacies in the existing legal framework concerning the diverse and ever-evolving forms of online sexual abuse that children are exposed to. These gaps are evident not only in the laws themselves but also in their implementation, underscoring the need for urgent improvements in child protection against online sexual abuse.

In today's rapidly evolving digital landscape, the urgent need to safeguard children from online sexual abuse in India has never been more pressing. While the nation has established a legal framework aimed at child protection, a comprehensive evaluation reveals significant deficiencies in both the existing laws and their practical application, underscoring the critical importance of bridging these gaps. At the heart of this issue is the Juvenile Justice (Care & Protection of Children) Act, a landmark legislation designed to bring India's legal framework in line with international standards. However, it is conspicuously silent on the provision of aftercare services for victims of online child abuse. This gaping omission leaves victims without the essential support and rehabilitation necessary for their recovery, a vital component in the comprehensive child protection landscape. Aftercare services play a pivotal role in helping survivors cope with the trauma and rebuild their lives. Without these services, the legal framework falls short of its intended goal.

Further exacerbating the issue is the absence of specific legal provisions to address child-on-child abuse in the digital realm, leaving a significant and problematic legal void. These cases, which often involve minors as both perpetrators and victims, require a nuanced response that takes into account the age and maturity of the individuals involved while still holding the wrongdoers accountable.[11] Without these tailored provisions, child-on-child abuse cases risk going unaddressed, leaving victims without the recourse and protection they desperately need.

Moreover, while the Juvenile Justice Act mandates the establishment of special Juvenile Police Units in every district, this critical directive remains largely unimplemented in many states, hampering effective responses to child abuse cases. These specialized units are designed to ensure a child-friendly legal process, but their absence leaves a significant gap in the child

[11] Human Rights Watch, Breaking the Silence, Child Sexual Abuse in India, 2013 Report

protection framework. Additionally, the requirement for each police station to designate 2-3 child welfare officers is often neglected, contributing to the shortage of specialized care for child abuse cases. This neglect further compounds the challenges faced by young victims of online sexual abuse in seeking help and justice.[12]

The misuse of cybercafés for organized child trafficking and cyber pornography adds another layer of complexity to the child protection landscape. Despite the existence of the IT (Cybercafé Guidelines) from 2011, authorities have failed to conduct regular monitoring of these facilities. As a result, they have become hotspots for criminal activities involving children. This glaring enforcement gap allows cybercriminals to exploit the anonymity of cybercafés for illicit purposes, putting children at risk.

The enforcement issues do not stop there. Section 69A of the Information Technology Act empowers the Central Government to block websites on grounds of public order. However, the Computer Emergency Response Team has failed to proactively block and filter pornographic websites, even though cyberpornography is illegal in India. The absence of clear due diligence requirements for intermediaries responsible for prefiltering websites hosting child pornographic or adult content further complicates the issue. This legal ambiguity leaves room for exploitation, allowing harmful content to circulate online.

In summary, the existing legal framework in India for safeguarding children from online sexual abuse reveals critical deficiencies, necessitating both legal amendments and an enhanced focus on practical implementation to ensure children's safety in the digital age. It is imperative that comprehensive child protection laws are put into place, that agencies are adequately resourced and trained to address online sexual abuse, and that the enforcement of these laws is prioritized to provide children with a safe digital environment.

Furthermore, India's obligations as a signatory to the Convention on the Rights of the Child demand that it take swift action to protect children from online sexual abuse. The Integrated Child Protection Scheme, while a significant step in the right direction, must extend its focus to include protecting children from online exploitation. India's non-signatory status to the Cybercrime Convention poses challenges in addressing cross-border cybercrimes targeting children, and the nation must consider aligning itself with international efforts to combat these crimes.

[12] Study of Child Abuse, India 2007, Retrieved from http://wcd.nic.in/childabusing.pdf

To address these deficiencies effectively, a multi-stakeholder approach is essential, involving legislators, parents, educators, NGOs, law enforcement, the private sector, and internet service providers in a Public-Private Partnership (PPP) model. It is imperative to eliminate the existing legal inadequacies, rectify inconsistencies, and ensure the laws are implemented effectively. To achieve this, government bodies must formulate appropriate policies and schemes to prevent and combat online child sexual abuse, accompanied by regular monitoring and efficient coordination through the established machinery. The government plays a pivotal role in orchestrating these efforts to create a safer online environment for children in India.

In conclusion, protecting children from online sexual abuse is a shared responsibility that encompasses legislation, enforcement, and international cooperation. The evolving digital landscape necessitates constant vigilance and adaptation to ensure that the nation's children are kept safe from harm. Addressing these legal gaps and implementing effective child protection measures is not just a legal and moral duty but a crucial step in securing India's digital future children in the digital age.

V. *Conclusion*

The digital age has brought about a revolution in the way we connect, communicate, and share information. While these advancements have enriched our lives, they have also exposed children to unprecedented risks in the online world. This paper has delved into the legal framework concerning child protection in the digital age in India, with a particular focus on child pornography, grooming, cyberbullying, and various forms of sexual harassment.

The analysis revealed that while India has made significant legislative strides in addressing these challenges, critical gaps and inconsistencies persist. The legal framework is a patchwork, with different laws and regulations addressing various aspects of online child protection. This fragmented approach leaves room for ambiguities, overlaps, and difficulties in practical implementation.

Child pornography and grooming, for instance, are addressed in the Information Technology Act and the Protection of Children from Sexual Offences (POCSO) Act. However, discrepancies in definitions and penalties between these laws create inconsistencies and hinder a comprehensive approach to these issues. Cyberbullying, a significant concern in the digital age, lacks a clear legal definition in Indian law. While some provisions can be applied, the absence of specific legislation addressing child sex abuse acts leaves a critical gap in addressing this form of harassment.

Practical implementation of child protection laws faces its own set of challenges. Aftercare services for victims of online child abuse are largely absent, specialized police units remain unimplemented, and the misuse of technology for child trafficking and cyber pornography continues due to inadequate monitoring. These issues are compounded by the failure to proactively block and filter pornographic websites. To bridge these gaps and create a robust child protection framework, a multi-stakeholder approach is imperative. Legislators, parents, educators, NGOs, law enforcement, the private sector, and internet service providers must collaborate in a Public-Private Partnership (PPP) model. The government must take the lead in formulating policies, providing resources, and ensuring effective coordination and monitoring.

In conclusion, protecting children in the digital age is a shared responsibility. The evolving digital landscape requires constant vigilance and adaptation to ensure the safety of children online. Addressing legal gaps, implementing effective child protection measures, and prioritizing international cooperation are not just legal and moral duties; they are essential steps in securing India's digital future and ensuring the well-being of its children. A comprehensive, coherent, and adaptable legal framework is the foundation upon which a safer online environment for India's children can be built.