

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 8 | Issue 2
2025

© 2025 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Tackling Online Child Exploitation in India: Legal Frameworks, Investigative Strategies, and Jurisdictional Challenges in Enforcing Cybercrime Laws

PARUL CHAUHAN¹, DR. MONIKA RASTOGI² AND MOHINI TANEJA³

ABSTRACT

The worrying rise of child exploitation crimes, coupled with child exploitation and abuse in the digital world in India, has left investigators with a big problem as well as the need for a review of laws. Over the years, even with multiple pieces of legislation like the Protection of Children from Sexual Offences (POCSO) Act, 2012 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, the grey area of child exploitation continues to spread in the digital space owing to the diverse threats posed by technology and complexities involving jurisdiction. The study examines the legal provisions and investigative mechanisms that address online child abuse and exploitation while also examining the jurisdictional complexity of cross-jurisdictional cybercrimes.

The present study aims to (i) understand the effectiveness of existing legal instruments (ii) evaluate the role of law enforcement agencies in investigating online occurrences of child exploitation (iii) analyse the intermingling of national and international legal systems and (iv) investigate the challenges caused due to the absence of uniformity in jurisdictional enforcement of cyber-crime laws. The methods used will be doctrinal study, case law analysis, and interviews of related stakeholders enforced on law, cybercrime units, and experts in the field of authority.

This study is aimed at adding to the body of work in the legal field that is addressing the need for the betterment of India's existing legal framework for the prevention of India in tackling cybercrimes demonstrating child exploitation. It will provide recommendations on how to better coordinate national and international agencies, potential new legislation, and best practices for effective cybercrime investigations. The national significance of this study is that it would add to the knowledge base as to the challenges and opportunities that face

¹ Author is a LLM Student at School of Law, Lingayas Vidyapeeth, Nachauli Jasana Road, Old Faridabad, Faridabad Haryana, India.

² Author is a Sr. Professor & Head at School of Law, Lingayas Vidyapeeth, Nachauli Jasana Road, Old Faridabad, Faridabad Haryana, India.

³ Author is an Assistant Professor at School of Law, Lingaya's Vidyapeeth, Nachauli Jasana Road, Old Faridabad, Faridabad Haryana

those who seek to combat online child exploitation so that policymakers and law enforcement will have a stronger framework from which to strengthen the national cybercrime response.

Keywords: *Cyber Crime, Child Exploitation, Sexual offences.*

I. INTRODUCTION

The swift growth of the digital realm in the last twenty years has yielded substantial advantages and considerable obstacles. The internet, initially a medium for communication and information dissemination, has now evolved into an integral component of daily existence, offering individuals unparalleled opportunities to connect, work, study, and participate in diverse online activities. India's internet user base has surged, exceeding 600 million individuals and establishing it as one of the largest populations of internet users globally. Consequently, digital platforms, including social media networks, online gaming, and peer-to-peer messaging services, have become integral to daily life, particularly for children and young adults. Nevertheless, in conjunction with these favourable advancements, the digital revolution has also facilitated the emergence of novel forms of criminal activity. One of the most alarming and widespread crimes enabled by the internet is online child exploitation. This term includes various criminal activities that involve the abuse and exploitation of minors for sexual purposes in the digital realm. The problem of online child exploitation in India has emerged as a significant concern for policymakers, law enforcement agencies, and civil society. The rising incidence of online child abuse cases underscores the pressing necessity for a thorough response. With the increasing internet penetration rate, particularly among children and adolescents, the associated risks escalate, fostering an environment conducive to exploitation.

India has experienced a swift increase in cybercrimes in recent years, with online child exploitation emerging as one of the most concerning categories of offences. The nation's youth demographic, comprising millions of children with access to smartphones and the internet, has rendered them especially susceptible to online predators. Digital platforms, including Facebook, Instagram, WhatsApp, and numerous online gaming applications, offer accessible and frequently anonymous environments for perpetrators to exploit children. The implementation of end-to-end encrypted communication channels has rendered it progressively challenging for law enforcement agencies to monitor and intercept these activities.

(A) Objective of the research

The study will specifically:

- To assess the sufficiency of current legal frameworks.
- To examine the investigative methodologies utilised by law enforcement agencies.
- To examine the jurisdictional complexities associated with investigating cybercrimes.

(B) Literature Review

Several connected theories that offer a basis for understanding the difficulties in tackling online child exploitation form the theoretical framework for this research. Among these theories are those of criminological theories of cybercrime, child rights, and the junction of law and technology.

- Srivastava (2017), for instance, examines the provisions of India's Protection of Children from Sexual Offences (POCSO) Act about online child sexual abuse and child pornography, so highlighting both its strengths and shortcomings. The study points up legal gaps, mostly in relation to cyber grooming and online trafficking where the law is either silent or vague. Nair (2018) also assesses the Information Technology Act, 2000's protection of children from online harm. She comes to the conclusion that although the IT Act criminalises the creation, distribution, and possession of child pornography, it does not sufficiently handle more modern techniques of exploitation including grooming via social media or live streaming platforms.
- International Cooperation and Jurisdictional Issues: Within the framework of international cybercrime, research on the complexity of jurisdictional challenges has been especially important. In 2021 Singh and Kumar investigate how international legal instruments including the Budapest Convention on Cybercrime and Mutual Legal Assistance Treaties (MLATs) might assist India in tackling cross-border online child exploitation. The study draws attention to India's challenges gathering proof from outside of its borders and punishing offenders who operate from elsewhere. The writers contend that the difficulties in combating transnational crimes like online child exploitation result from a lack of coordination between international law enforcement agencies and legal ambiguities in Indian cybercrime laws.

(C) Research Methodology

This study adopts a **doctrinal research methodology**, which is commonly used in legal research to analyze and interpret existing laws, regulations, judicial decisions, and scholarly works. Doctrinal research focuses on the identification, interpretation, and evaluation of legal texts to understand the framework of laws and their application in specific areas of concern.

This research methodology is particularly suitable for examining the legal frameworks and principles associated with online child exploitation, as well as investigating the effectiveness of existing legal mechanisms and the challenges in their enforcement.

II. LEGAL FRAMEWORKS IN INDIA TACKLING ONLINE CHILD EXPLOITATION

India has made substantial progress in establishing legal frameworks to address online child exploitation. These statutes aim to safeguard children from maltreatment, ensure accountability for offenders, and establish frameworks for investigation and prosecution. The principal legal provisions pertinent to online child exploitation in India encompass:

- **Protection of Children from Sexual Offences Act, 2012:** The POCSO Act was established to safeguard children from sexual abuse, sexual harassment, and pornography. It offers extensive legal safeguards for children by prohibiting multiple forms of child sexual exploitation. Under the POCSO Act, any involvement of a child in the production, distribution, or possession of child pornography constitutes an offence subject to imprisonment and a monetary penalty. The law underscores the necessity of protecting the child's identity and requires the implementation of child-friendly protocols during investigation and prosecution.
- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.** These regulations, governed by the Information Technology Act, 2000, delineate protocols for safeguarding individuals' online privacy, especially concerning sensitive personal information. While not solely dedicated to child exploitation, these regulations establish the legal framework for managing personal data, thereby enhancing the safety of the internet for children.
- **The Information Technology Act of 2000:** This legislation is fundamental to India's cybercrime statutes and addresses various offences, including cyberbullying, hacking, and online exploitation. According to Section 67B of the IT Act, the creation, distribution, and possession of child pornography constitute criminal offences. Section 66E of the Act pertains to privacy violations, which may encompass cases of child exploitation related to digital abuse.
- **Indian Penal Code, 1860.** Multiple provisions of the IPC may be applied in instances of online child exploitation. Sections 354C and 354D address stalking and voyeurism, offences that are progressively perpetrated through digital platforms. Provisions under Sections 376 (rape) and 377 (unnatural offences) are applicable to instances of online

child sexual exploitation.

- **The Juvenile Justice (Care and Protection of Children) Act, 2015.** This act primarily emphasises the welfare and rehabilitation of children requiring care and protection, while also addressing the legal aspects concerning children who are victims of abuse. The Juvenile Justice Act provides a structure for addressing child victims, safeguarding them from re-victimization throughout legal processes.
- **The Cyber Crime Investigation and Coordination Centre (C-4i)** was established by the Indian government to address cybercrimes, particularly online child exploitation. The center facilitates the coordination of cybercrime investigations across states and provides technical assistance for the collection of digital evidence.

Notwithstanding the existence of these legal provisions, obstacles persist in the enforcement of these laws. The swift expansion of internet usage, the advancement of novel technologies, and the rise of encrypted communication channels have hindered law enforcement agencies' ability to track cybercriminals. The inadequate training and resources in digital forensics for police forces and judicial officers have impeded the efficacy of investigations.

III. CHALLENGES IN ENFORCING CYBER CRIME

Despite India's establishment of a legal framework to combat cyber crime, numerous challenges impede its enforcement. The challenges encompass:

- **Cross-Border Jurisdictional Complications:** Online child exploitation frequently entails offenders, victims, and evidence dispersed across various nations, resulting in jurisdictional challenges. The internet is a worldwide platform, and cybercrimes often surpass national borders. India's legal system encounters challenges in cooperating with other nations regarding the investigation and prosecution of online child exploitation, attributable to disparities in legal frameworks and the lack of definitive international protocols for cybercrime investigations.
- **Technological Barriers:** The swift progression of technological innovation frequently surpasses law enforcement's capacity to adapt. The utilisation of encrypted communications, virtual private networks (VPNs), and anonymous online transactions complicates the efforts of investigators to identify perpetrators. Cybercriminals frequently employ tools that obscure their identity and location, thereby complicating the collection of digital evidence.
- **Resource Limitations:** Law enforcement agencies in India frequently lack the requisite

resources and expertise to adequately investigate and prosecute cases of online child exploitation. Digital forensics, essential in these instances, necessitates specialised expertise and apparatus. Many police departments, however, are inadequately funded and lack the necessary infrastructure to manage the rising incidence of cybercrime cases.

- **Public Awareness and Reporting Deficiencies:** There exists a deficiency in awareness among the public and law enforcement regarding the magnitude and extent of online child exploitation. A multitude of cases remain unreported, either due to victims' unawareness of their exploitation or the societal stigma associated with sexual abuse. Furthermore, parents and guardians frequently lack the expertise to adequately oversee their children's online behaviours.

IV. PRACTICAL IMPLEMENTATIONS

1. **Strengthening Legal Frameworks:** Based on the research findings, one practical implementation could be the introduction of new legal provisions to address emerging forms of online child exploitation. For instance, specific legal provisions could be introduced to address the growing threat of online grooming, live-streaming abuse, and the exploitation of children through online gaming platforms. A more comprehensive legal framework would enable law enforcement agencies to take swift action in these emerging areas.
2. **Improving Digital Forensics Capabilities:** Law enforcement agencies will be better equipped to investigate online child exploitation cases through the implementation of enhanced digital forensics training and the acquisition of specialized tools. The research will identify the critical areas in which law enforcement requires training, such as data recovery, cyber surveillance, and the preservation of digital evidence. A national strategy to improve digital forensics capabilities could be developed, allowing law enforcement agencies across India to better combat online child exploitation.
3. **International Cooperation Initiatives:** The research will highlight the need for enhanced international cooperation in prosecuting online child exploitation, particularly in cases involving cross-border elements. Practical implementations could involve India's increased participation in international legal frameworks like the **Budapest Convention** and the expansion of bilateral and multilateral agreements on cybercrime. This would facilitate smoother cooperation in sharing evidence and prosecuting offenders across jurisdictions.
4. **Public Awareness and Collaboration:** Another practical implication of the research is

the promotion of public awareness regarding online child exploitation. Recommendations could include the establishment of awareness campaigns targeting children, parents, educators, and internet service providers to prevent online exploitation. Additionally, the research will advocate for greater collaboration between government agencies, non-governmental organizations, technology companies, and civil society to create a more cohesive response to online child exploitation.

5. **Judicial Reforms:** In light of the findings, the research will suggest reforms to the judicial process to expedite the prosecution of online child exploitation cases. These reforms could include the creation of specialized courts for cybercrimes, including online child exploitation cases, to ensure faster trial processes and more consistent application of the law.

V. CONCLUSION

In conclusion, tackling online child exploitation in India requires a multifaceted approach, involving the strengthening of legal frameworks, the enhancement of investigative strategies, and the overcoming of significant jurisdictional challenges. The existing legal provisions, such as the **Protection of Children from Sexual Offences (POCSO) Act** and the **Information Technology Act, 2000**, provide a foundation for combating child exploitation in the digital realm. However, the rapid evolution of technology and the increasing complexity of cybercrimes highlight the urgent need for legal reforms to address emerging forms of abuse, such as cyber-grooming and live-streaming exploitation.

Investigative strategies, including digital forensics and international cooperation, are crucial in identifying and prosecuting offenders. Yet, limitations in resources, technical expertise, and cross-border legal cooperation hinder the effectiveness of these efforts. Jurisdictional challenges further complicate the enforcement of laws, particularly when perpetrators operate from different countries with varying legal systems and standards of cooperation.

To effectively address online child exploitation, India must prioritize the integration of modern technology into law enforcement practices, improve training and resources for law enforcement agencies, and enhance international collaboration. Moreover, legislative reforms must address the evolving nature of cybercrimes, ensuring that Indian laws remain robust and adaptable. By bridging the existing gaps in legal frameworks, investigative strategies, and international cooperation, India can better safeguard its children from the growing threat of online exploitation.

VI. REFERENCES

(A) Books and Articles:

- **Bhatia, V. K.** (2016). *Cyber Law: A Guide for the New Economy*. Oxford University Press.
- **Lynch, R.** (2017). *Online Child Exploitation and the Law: Challenges and Advances*. Cambridge University Press.
- **Mitra, S.** (2020). "The Protection of Children from Sexual Offences (POCSO) Act, 2012: Gaps and Challenges in the Indian Context." *Indian Journal of Law and Social Sciences*, 9(2), pp. 21-36.
- **Rao, K. V.** (2019). "Legal Challenges in Combating Cybercrime in India." *Indian Journal of Law and Technology*, 3(1), pp. 55-73.

(B) Legal and Governmental Sources:

- **Government of India.** (2012). *Protection of Children from Sexual Offences (POCSO) Act, 2012*.
- **Ministry of Electronics and Information Technology (MeitY).** (2020). *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*.
- **National Commission for Protection of Child Rights (NCPCR).** (2021). *Child Protection and Online Safety: A Report on Cybercrimes Affecting Children in India*.

(C) International Conventions and Reports:

- **United Nations.** (1989). *Convention on the Rights of the Child (CRC)*.
- **Council of Europe.** (2001). *Convention on Cybercrime (Budapest Convention)*.
- **Interpol.** (2019). *Global Threat Assessment on Online Child Exploitation*.
- **Europol.** (2020). *The Threat of Online Child Sexual Abuse: Trends and Countermeasures*.

(D) Research Papers and Reports:

- **Das, S.** (2021). "Addressing Online Child Exploitation: Legal and Technical Challenges in India." *Journal of Cyber Security and Law*, 5(3), pp. 78-92.
- **Kumar, R. & Sharma, M.** (2020). "Cybercrimes and the Protection of Children: The Role of Law Enforcement in India." *Journal of Cyberlaw & Technology*, 7(4), pp. 112-

130.

- **UNICEF.** (2019). *Child Online Protection in India: A Comprehensive Study.*
- **Asian Centre for Human Rights (ACHR).** (2018). *Online Child Sexual Abuse in India: Legal and Socio-Cultural Dimensions.*

(E) Websites and Online Resources:

- **Cyber Crime Cell, Ministry of Home Affairs, Government of India.** (2021). *Cyber Crime and Prevention of Online Child Exploitation.*
- **Internet Watch Foundation (IWF).** (2020). *Annual Report on Global Child Sexual Abuse Content Online.*
- **The Digital Empowerment Foundation (DEF).** (2021). *Online Child Protection in India: Challenges and Strategies.*
