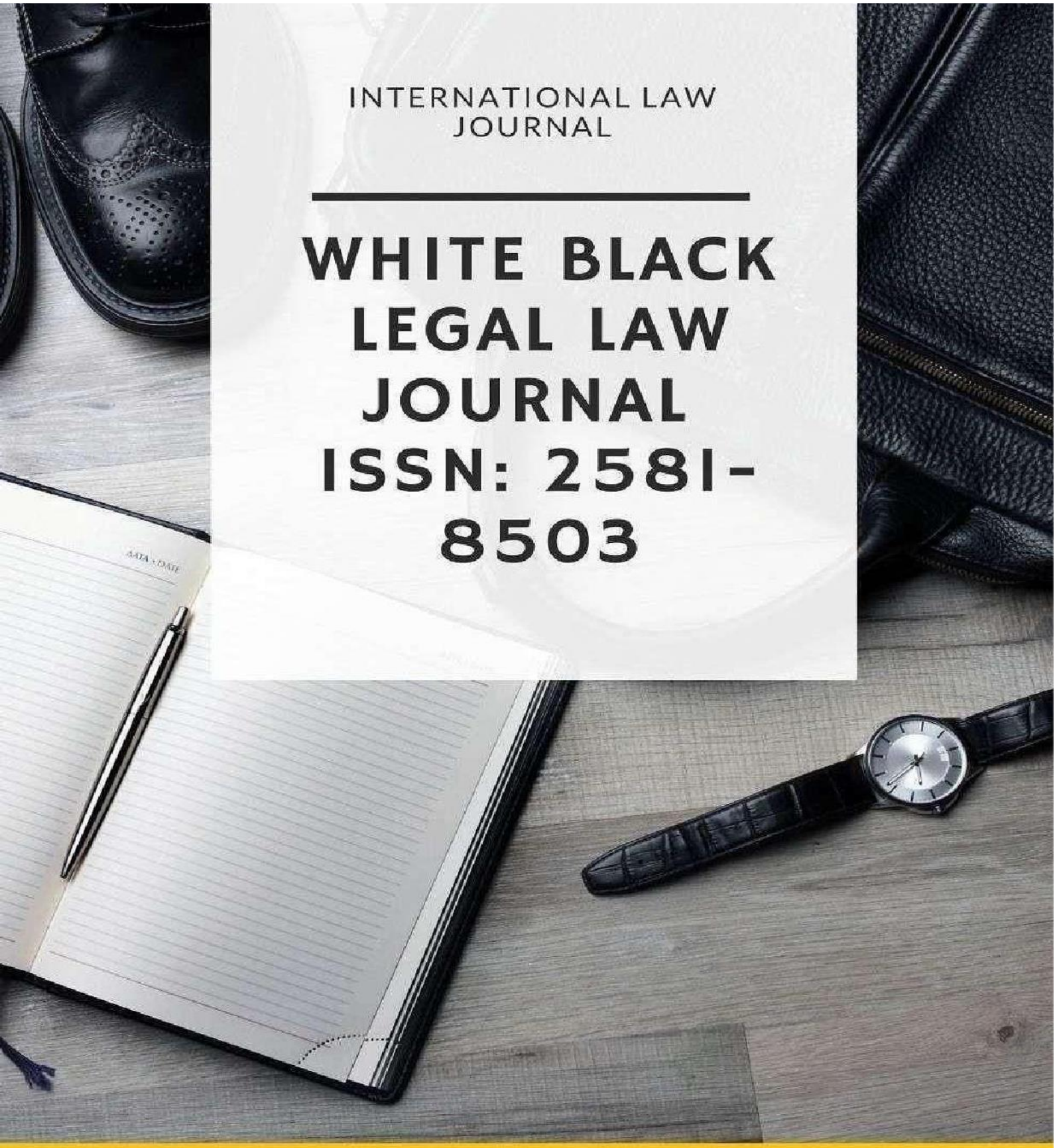

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 7 | June 2026 ISSN: 2581-8503

ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE: STRENGTHENING CYBER LAW ENFORCEMENT MECHANISMS

AUTHORED BY - DEEPAK CHAHAL
Punjabi University, Patiala

Abstract

Online Child Sexual Exploitation and Abuse (OCSEA) represents one of the most grievous violations of children's rights in the digital age, combining sexual exploitation, psychological harm, and the perpetual re-victimization inherent in the circulation of child sexual abuse material (CSAM) on digital platforms. India, with one of the world's largest and fastest-growing internet user populations particularly among youth faces acute challenges in preventing, detecting, and prosecuting OCSEA. The existing legal framework, comprising the Protection of Children from Sexual Offences Act, 2012 (POCSO Act), the Information Technology Act, 2000 (IT Act), and the Indian Penal Code (IPC), provides a multi-layered but fragmented legal architecture that struggles to keep pace with the evolving technological landscape of online child sexual exploitation. This paper undertakes a comprehensive analysis of the legal framework governing OCSEA in India, the cyber law enforcement mechanisms deployed to combat it, and the structural, technological, and jurisdictional challenges that impede effective law enforcement. The paper examines the roles of intermediaries, the challenges of encryption and the dark web, international cooperation frameworks, and the jurisprudential treatment of OCSEA by Indian courts. Drawing on comparative frameworks from the European Union, the United States, the United Kingdom, and Australia, the paper argues that effective combating of OCSEA requires a multi-stakeholder approach involving legislative reform, capacity building in law enforcement, meaningful intermediary accountability, enhanced international cooperation, and robust child protection systems. Concrete reform recommendations are presented.

Keywords: *online child sexual exploitation and abuse, OCSEA, CSAM, POCSO Act, IT Act, cyber law, child pornography, grooming, dark web, intermediary liability, India, cyber enforcement*

1. Introduction

The proliferation of digital technology and internet connectivity has created unprecedented opportunities for education, communication, and development. It has also created new vectors for the sexual exploitation and abuse of children, generating a global crisis that demands urgent and sustained attention from legislators, law enforcement agencies, technology companies, civil society, and the judiciary. Online Child Sexual Exploitation and Abuse encompasses a spectrum of conduct: the production, distribution, and possession of child sexual abuse material (CSAM); grooming and enticement of children for sexual purposes through online platforms; live-streaming of child sexual abuse; sexual extortion (sextortion); and the exposure of children to sexual content without consent.

India presents a particularly complex and urgent context for addressing OCSEA. With over 800 million internet users and rapidly growing smartphone penetration, including among children and adolescents, India is among the countries most vulnerable to online child sexual exploitation. The National Crime Records Bureau (NCRB) data for 2022 showed a dramatic increase in registered POCSO cases involving online elements. The Internet Watch Foundation and similar bodies have identified India as a significant source and destination country for CSAM. The COVID-19 pandemic and the consequent increase in screen time among children accelerated the growth of online risk.

Despite the gravity of the threat, the legal and enforcement framework for combating OCSEA in India faces significant challenges: definitional gaps in legislation; inadequate technological capacity in law enforcement; the challenges of investigating crimes on encrypted platforms and the dark web; limitations in intermediary accountability; and weak international cooperation mechanisms. These challenges are compounded by social taboos surrounding the discussion of child sexual abuse, the stigma faced by survivors, and the inadequacy of support services for child victims.

This paper provides a critical analysis of the legal framework and enforcement mechanisms for OCSEA in India. Section 2 outlines the methodology. Section 3 sets out research objectives and questions. Section 4 reviews the literature. Section 5 constitutes the analytical body of the paper. Section 6 presents conclusions and recommendations.

2. Methodology

This research employs a doctrinal legal methodology, analyzing the primary legislative sources POCSO Act, 2012; IT Act, 2000 and its 2008 Amendments; IPC; IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 alongside significant judicial decisions and parliamentary committee reports. The analysis is supplemented by a comparative examination of the legal frameworks of the European Union (particularly the EU Directive on Combating Sexual Abuse and Sexual Exploitation of Children and Child Pornography), the United States (PROTECT Act, CIPA, EARN IT Act debate), the United Kingdom (Online Safety Act, 2023), and Australia (Online Safety Act, 2021).

Secondary sources include reports of international bodies such as UNICEF, ECPAT International, the Internet Watch Foundation, the National Center for Missing and Exploited Children (NCMEC), and the WeProtect Global Alliance. Government reports from the Ministry of Home Affairs, the National Commission for Protection of Child Rights (NCPCR), and the CBI are also drawn upon. The paper also references empirical studies on OCSEA prevalence, victim impact, and law enforcement challenges.

Given the sensitive nature of the subject matter, the research does not involve direct engagement with victims or survivors. Anonymized case data from published court judgments and research studies is used throughout.

3. Research Objectives and Questions

3.1 Objectives

The objectives of this research are: (i) to critically analyze the legal framework governing OCSEA in India, identifying definitional gaps and overlaps; (ii) to evaluate the effectiveness of cyber law enforcement mechanisms in detecting, investigating, and prosecuting OCSEA; (iii) to examine the legal obligations and liability of intermediaries in relation to OCSEA; (iv) to assess the challenges posed by encryption and the dark web for law enforcement; (v) to analyze India's participation in international cooperation frameworks for combating OCSEA; and (vi) to formulate evidence-based recommendations for strengthening the legal and enforcement framework.

3.2 Research Questions

1. Does the existing legal framework under POCSO, the IT Act, and IPC adequately criminalize the full spectrum of OCSEA conduct, including emerging forms such as AI-generated CSAM and live-streaming?
2. What are the principal technological, institutional, and jurisdictional challenges faced by Indian law enforcement in investigating and prosecuting OCSEA?
3. Are the intermediary obligations under the IT (Intermediary Guidelines) Rules, 2021 adequate to address OCSEA on digital platforms?
4. How can India's international cooperation framework for OCSEA investigation be strengthened?

4. Literature Review

The literature on OCSEA spans criminology, legal scholarship, child protection studies, and computer science. The interdisciplinary nature of the problem necessitates engagement with a diverse body of scholarship.

Quayle and Taylor (2002) conducted pioneering research on the online sexual exploitation of children, focusing on the psychological profiles of offenders and the role of child sexual abuse material in facilitating both individual offending and the development of offending networks. Their work established that CSAM serves not only as a record of abuse but as a tool for grooming new victims and validating offending behavior within online communities (Quayle & Taylor, 2002, pp. 331-335). This insight has been foundational to subsequent legal and policy responses that have focused on both the supply and demand sides of CSAM.

In the Indian context, Ghosh and Bhattacharya (2014) provided the first systematic legal analysis of the POCSO Act, 2012 in the context of online child sexual exploitation. They identified critical definitional gaps, noting that while Section 13 of POCSO criminalizes the use of children for pornographic purposes, the Act does not adequately address distribution, transmission, or foreign-hosted CSAM. They also highlighted the inadequacy of the Act's provisions on child witness protection in the context of online abuse cases, where the evidentiary challenges are compounded by technical complexity (Ghosh & Bhattacharya, 2014, pp. 55-59).

Bajpai (2017) examined the interface between POCSO and the IT Act in the enforcement of OCSEA laws, finding significant legal uncertainty arising from the overlapping and sometimes conflicting provisions of the two statutes. Bajpai argued that the absence of a unified legislative framework for online child sexual exploitation created enforcement gaps that offenders could exploit, and that the jurisdictional ambiguity between state police and central agencies compounded the problem (Bajpai, 2017, pp. 88-93).

Sharma (2019) conducted empirical research on the investigation of online child exploitation cases by state police agencies in India, finding that most agencies lacked the specialized digital forensics capability required to investigate OCSEA effectively. Sharma found that fewer than thirty percent of state police forces had dedicated cyber cells with trained personnel, that digital evidence was frequently mishandled resulting in its inadmissibility in court, and that most investigators lacked the technical knowledge to trace offenders on encrypted platforms or the dark web (Sharma, 2019, pp. 112-118).

The role of technology companies in combating OCSEA has been analyzed by several scholars. Laidlaw (2015) examined the legal and ethical obligations of internet intermediaries in relation to CSAM, arguing that while intermediaries bear significant moral responsibility for the distribution of CSAM on their platforms, the imposition of legal liability must be carefully calibrated to avoid the collateral censorship of legitimate speech. Laidlaw advocated for a notice-and-takedown framework coupled with mandatory CSAM detection technology as the optimal regulatory approach (Laidlaw, 2015, pp. 295-300).

The emergence of AI-generated CSAM has been addressed by more recent scholarship. Europol (2022) and the Internet Watch Foundation (2023) have documented the growing volume of AI-generated child sexual abuse imagery and have raised urgent questions about whether existing legal frameworks which often focus on the exploitation of identifiable real children are adequate to address synthetic CSAM. McGlynn and Rackley (2022) argued that synthetic CSAM normalizes child sexual abuse, creates demand for real CSAM, and must be criminalized unequivocally regardless of the absence of an identifiable victim (McGlynn & Rackley, 2022, pp. 45-49).

The global dimensions of OCSEA have been analyzed by Muir (2005) and Edwards (2016). Muir's early work on the global dimensions of CSAM documented the emergence of

international networks for the production and distribution of CSAM and the need for coordinated international law enforcement responses. Edwards analyzed the challenges of mutual legal assistance in OCSEA investigations, noting that the traditional MLAT (Mutual Legal Assistance Treaty) framework is too slow for the fast-moving digital environment and that new mechanisms for real-time data sharing between law enforcement agencies are urgently needed (Edwards, 2016, pp. 78-84).

The WeProtect Global Alliance (2021) has published comprehensive global threat assessments and model national response frameworks for OCSEA, which provide the most current and authoritative overview of the global landscape of online child sexual exploitation. Their framework for national action, encompassing legislation, law enforcement capacity, industry obligations, child protection systems, and international cooperation, provides a useful template for evaluating national frameworks including India's.

Kumar and Reddy (2022) examined the implementation of the NCPCR's CyberTipline and the Cybercrime Prevention against Women and Children (CCPWC) scheme in India, finding significant gaps in the triage and investigation of CSAM reports, particularly in non-metropolitan areas. They found that the absence of standardized protocols for handling CSAM evidence across states created significant disparities in investigation quality and prosecution success rates (Kumar & Reddy, 2022, pp. 67-74).

5. Analysis

5.1 Legal Framework: POCSO Act, 2012

The Protection of Children from Sexual Offences Act, 2012 is the primary legislation governing child sexual abuse in India. Chapter II defines the principal sexual offences against children, including penetrative sexual assault (Section 3), aggravated penetrative sexual assault (Section 5), sexual assault (Section 7), aggravated sexual assault (Section 9), sexual harassment of a child (Section 11), and the use of a child for pornographic purposes (Section 13). The Act defines 'child' as any person below the age of eighteen years.

Section 13 criminalizes the use of a child in any form of media for the purpose of sexual gratification, including producing, distributing, or showing child pornography. Section 14 prescribes enhanced penalties when a person who commits an offence under Section 13 uses electronic media. Section 15 specifically addresses the storage of CSAM, criminalizing the

downloading, browsing, or possession of child pornography. The 2019 Amendment to POCSO strengthened Section 15 by creating a new offence of failure to delete or report CSAM and by increasing penalties across several provisions.

Despite these provisions, POCSO has several limitations in the online context. The Act does not explicitly address online grooming the process by which an offender cultivates a relationship with a child for the purpose of sexual exploitation. Section 11 criminalizes 'sexual harassment' in broad terms that could encompass online grooming, but the absence of a specific provision creates evidentiary challenges. The Act also does not specifically address sextortion the coercion of children through the threatened disclosure of intimate images which has emerged as a significant and growing form of online child sexual exploitation.

5.2 Information Technology Act, 2000 and Cyber Provisions

The Information Technology Act, 2000, as amended in 2008, provides supplementary legal tools for combating OCSEA. Section 67B specifically criminalizes the publication, transmission, or creation of material in electronic form depicting children in sexually explicit acts, and the browsing, downloading, or possession of such material. Section 67B carries enhanced penalties compared to the corresponding POCSO provisions, prescribing imprisonment of up to five years and a fine on first conviction, and up to seven years on subsequent conviction.

Section 66E of the IT Act criminalizes the violation of privacy through the capturing and publishing of intimate images without consent. While not specifically directed at children, this provision is relevant to OCSEA scenarios involving the non-consensual sharing of children's intimate images. Section 66F addresses cyber terrorism, which may be applicable in cases where OCSEA is organized and conducted by criminal networks at scale.

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose significant obligations on social media intermediaries and other platforms to detect, remove, and report CSAM. Rule 3(1)(b)(ii) requires intermediaries not to host content that depicts children in sexually explicit acts. Rule 4(4) requires significant social media intermediaries those with more than five million users in India to deploy automated tools to identify CSAM. These provisions represent a significant step towards meaningful intermediary accountability but raise concerns about implementation and over-removal.

5.3 Role of Intermediaries and Platform Accountability

Digital platforms social media networks, messaging applications, file hosting services,

and peer-to-peer networks are the primary vectors through which CSAM is produced, distributed, and accessed. The legal framework for intermediary accountability in India has evolved significantly over the past decade. Prior to the 2021 Rules, intermediaries enjoyed broad immunity from liability for third-party content under Section 79 of the IT Act, provided they exercised due diligence and complied with take-down notices.

The 2021 Rules shifted the paradigm by imposing proactive obligations on significant social media intermediaries to deploy technology specifically PhotoDNA and similar hash-matching tools to detect and remove known CSAM. The Rules also require intermediaries to appoint a Grievance Officer, a Chief Compliance Officer, and a Nodal Contact Person resident in India. Quarterly compliance reports are to be published. Non-compliance results in the loss of safe harbour protection under Section 79.

However, the Rules do not require end-to-end encrypted messaging platforms to implement CSAM detection, given the technical incompatibility of client-side scanning with end-to-end encryption. This creates a significant regulatory gap, as encrypted messaging platforms are widely used for sharing CSAM. The global debate over client-side scanning which would scan messages before encryption is live in India, with the NCPCR and Ministry of Home Affairs having raised the issue with major platforms, but no legislative resolution has been reached.

The National Center for Missing and Exploited Children (NCMEC) CyberTipline receives reports of CSAM from US-based technology companies and shares them with law enforcement globally, including India's CBI. The volume of CyberTipline reports relating to India has grown dramatically, from approximately 100,000 in 2017 to over 3 million by 2022. However, the capacity of Indian law enforcement to investigate and prosecute these leads has not kept pace with the volume of reports, resulting in a significant investigation backlog.

5.4 Law Enforcement Capacity and Challenges

Effective investigation of OCSEA requires specialized skills in digital forensics, open-source intelligence (OSINT), undercover online operations, and international cooperation. The current capacity of Indian law enforcement to conduct such investigations is severely limited. Most state police forces lack dedicated cybercrime units with the equipment, training, and staffing necessary to investigate OCSEA effectively. The CBI's Online Child Sexual Exploitation Unit, while specialized, has limited capacity relative to the scale of the problem.

Digital forensic evidence presents particular challenges in the Indian legal system. Courts have struggled with the admissibility requirements for electronic evidence under

Section 65B of the Indian Evidence Act, which requires a certificate from the person responsible for the electronic device or system. In OCSEA cases where evidence is obtained from foreign servers through international cooperation, the Section 65B certification requirement can create insurmountable evidentiary hurdles.

The dark web accessible through anonymizing tools such as the Tor browser hosts significant volumes of CSAM in forums and marketplaces that are difficult to access and investigate. Indian law enforcement agencies have very limited capacity for dark web investigations, lacking both the technical expertise and the legal authority for certain investigative techniques used in comparable jurisdictions. The absence of explicit legislative authorization for undercover online operations creates legal uncertainty for investigators who engage in such techniques.

The rapid proliferation of AI-generated CSAM including 'deepfake' imagery and fully synthetic child sexual abuse content poses new challenges for both law enforcement and legislation. AI-generated CSAM may not involve the exploitation of a real, identifiable child, yet it normalizes child sexual abuse, is used in grooming, and is increasingly indistinguishable from real imagery. The current legal framework does not explicitly address synthetic CSAM, creating a potential legal gap that offenders may exploit.

5.5 International Cooperation Framework

OCSEA is inherently transnational: offenders, victims, servers, and financial flows frequently span multiple jurisdictions. Effective law enforcement requires robust mechanisms for international cooperation. India's international cooperation framework for OCSEA investigation relies primarily on Mutual Legal Assistance Treaties (MLATs) with approximately forty countries, informal cooperation through INTERPOL's channels and the Virtual Global Taskforce, and emergency data disclosure requests to technology companies under their terms of service.

The MLAT framework is widely recognized as inadequate for the digital age. The average time for processing an MLAT request in the United States the jurisdiction hosting the servers of most major social media platforms is reported to exceed ten months, far too slow for the fast-moving digital evidence environment where data may be deleted or overwritten within days or weeks of a request. The US CLOUD Act of 2018 provides a more expedited mechanism for government-to-government data sharing, and India has initiated but not yet concluded a CLOUD Act agreement with the United States.

India is a member of the WeProtect Global Alliance and the Virtual Global Taskforce,

multi-stakeholder international initiatives that facilitate the sharing of intelligence, best practices, and operational support in OCSEA investigations. India participates in INTERPOL's Operation Rescue and similar coordinated international operations targeting CSAM networks. However, India is not yet a party to the Budapest Convention on Cybercrime, which provides the most comprehensive international legal framework for cybercrime cooperation, including OCSEA. Accession to the Budapest Convention would significantly strengthen India's international cooperation capacity.

5.6 Child Victim Protection and Support

The legal framework for child victim protection in OCSEA cases is an essential complement to enforcement measures. POCSO Act provisions on the protection of child victims during investigation and trial including the designation of Special Courts, the appointment of support persons, and the in-camera trial requirement are positive but inadequately implemented. Research has documented that investigators and prosecutors frequently lack the training to conduct child-friendly interviews, and that Special Courts are not universally available or adequately resourced.

The perpetual re-victimization inherent in CSAM where images of abuse continue to circulate after the initial abuse has ended creates a distinct form of ongoing harm that the legal framework does not adequately address. The right of survivors to request removal of their images from online platforms is not explicitly codified in Indian law, though the NCPCR has issued guidelines in this regard. A legislative right to CSAM image removal, with corresponding obligations on intermediaries, would fill this gap.

5.7 Comparative Frameworks

The European Union's approach to OCSEA is anchored in Directive 2011/93/EU, which requires Member States to criminalize a comprehensive range of conduct including solicitation of children online, access to CSAM, and grooming. The EU proposal for a Child Sexual Abuse Regulation, debated since 2022, would impose mandatory CSAM detection obligations on online platforms, including encrypted messaging services, through client-side scanning a proposal that has been highly controversial from a privacy standpoint but reflects the seriousness with which the EU treats OCSEA.

The United States' legal framework comprises the PROTECT Act (2003), which criminalizes the production, distribution, and possession of CSAM including obscene visual depictions of minors even where no real child is identifiable; the CIPA (Children's Internet

Protection Act, 2000), which requires internet filtering in schools and libraries; and the EARN IT Act debate, which addresses end-to-end encryption and mandatory CSAM reporting. The US NCMEC CyberTipline model requiring technology companies to report CSAM to a designated body has been widely adopted and provides a model for India.

Australia's Online Safety Act, 2021 provides comprehensive powers to the eSafety Commissioner to require the removal of CSAM and other seriously harmful content, with enforceable standards for online service providers. The Commissioner's powers include the ability to investigate complaints, issue notices, and seek civil penalties for non-compliance a model that significantly exceeds the current enforcement capacity of India's NCPCR in the online safety domain.

6. Conclusion and Recommendations

The legal framework for combating OCSEA in India comprising POCSO, the IT Act, and the 2021 Intermediary Rules provides a foundation but is inadequate to address the full spectrum of online child sexual exploitation in the current technological environment. Significant gaps remain in the criminalization of emerging forms of OCSEA (grooming, sextortion, AI-generated CSAM), the technological capacity of law enforcement, the accountability of encrypted platforms, the international cooperation framework, and the support available to child survivors.

The following recommendations are presented: First, POCSO should be amended to explicitly criminalize online grooming, sextortion, and AI-generated CSAM, with definitions that are technology-neutral and future-proofed. Second, India should establish a dedicated national agency for online child safety with the powers of investigation, enforcement, and platform regulation modeled on Australia's eSafety Commissioner. Third, all law enforcement agencies investigating OCSEA should be required to meet minimum standards of digital forensic capability and training, with central funding for capacity building. Fourth, India should accede to the Budapest Convention on Cybercrime and expedite a CLOUD Act agreement with the United States to improve real-time data access for OCSEA investigations. Fifth, the NCPCR CyberTipline should be significantly expanded and resourced to triage and distribute CSAM reports to state and central agencies efficiently. Sixth, a statutory right to CSAM image removal should be codified, with corresponding obligations on intermediaries to respond within defined timeframes. Seventh, child survivor support services, including psychological

counseling, legal assistance, and image removal support, should be made available nationally and adequately funded.

The protection of children from sexual exploitation in the digital age is not merely a law enforcement challenge it is a fundamental test of whether society values the safety and dignity of its most vulnerable members. A comprehensive, adequately resourced, and internationally connected response framework is urgently needed, and the legal reform proposals advanced in this paper constitute a starting point for the necessary transformation of India's OCSEA response.

Bibliography

- Bajpai, A. (2017). Child rights in India: Law, policy and practice (3rd ed.). Oxford University Press.
- Edwards, L. (2016). From child protection to the fight against cybercrime: The global governance of CSAM. Journal of Internet Law, 19(10), 75-88.
- Europol. (2022). Online child sexual exploitation and abuse: Emerging trends. Europol Public Information Report.
- ECPAT International. (2020). Global monitoring status of action against commercial sexual exploitation of children: India. ECPAT.
- Ghosh, S., & Bhattacharya, D. (2014). POCSO Act and online child exploitation: A critical analysis. National Law University Delhi Law Review, 5(1), 48-65.
- Government of India. (2000). Information Technology Act, 2000. Ministry of Law and Justice.
- Government of India. (2012). Protection of Children from Sexual Offences Act, 2012. Ministry of Law and Justice.
- Government of India. (2021). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Ministry of Electronics and Information Technology.
- Internet Watch Foundation. (2023). Annual report 2022. IWF.
- Kumar, A., & Reddy, P. (2022). NCPCR CyberTipline: Capacity and challenges. Centre for Child Rights, Working Paper No. 14.
- Laidlaw, E. (2015). Regulating speech in cyberspace: Gatekeepers, human rights and corporate responsibility. Cambridge University Press.

- McGlynn, C., & Rackley, E. (2022). AI-generated child sexual abuse material: A critical appraisal of current and proposed legal responses. Child & Family Law Quarterly, 34(1), 39-56.
- Muir, D. (2005). Violence against children in cyberspace. ECPAT International.
- National Commission for Protection of Child Rights. (2021). Guidelines for prevention of and response to online child sexual exploitation. NCPCR.
- National Crime Records Bureau. (2022). Crime in India 2022. Ministry of Home Affairs, Government of India.
- Quayle, E., & Taylor, M. (2002). Child pornography and the internet: Perpetuating a cycle of abuse. Deviant Behavior, 23(4), 331-361.
- Sharma, N. (2019). Cybercrime investigation and child exploitation in India: Capacity assessment. Commonwealth Human Rights Initiative.
- UNICEF. (2020). Disrupting harm in India: Evidence on online child sexual exploitation and abuse. ECPAT International, INTERPOL, and UNICEF.
- United Nations. (1989). Convention on the Rights of the Child. United Nations.
- United Nations. (2000). Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography. United Nations.
- WeProtect Global Alliance. (2021). Global threat assessment 2021: Assessing the nature and scale of child sexual exploitation and abuse online. WeProtect.