DIGITAL EXPLOITATION OF CHILDREN IN INDIA: LEGAL CHALLENGES AND REFORMS

Rayana Afrin N

LL.B. LLB III[rd] Year VI[th] Semester, School of Law, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai | Under the Guidance of **Mrs. G. Uma Maheswari,** Assistant Professor, Department of Legal Studies, School of Law, VISTAS,

ABSTRACT

The rapid proliferation of internet access in India has fundamentally transformed the nature and scale of threats faced by children in digital spaces. Crimes such as online grooming, cyberbullying, child sexual abuse material (CSAM), sextortion, and digital trafficking have grown alongside increasing internet penetration, exposing millions of vulnerable minors to exploitation with impunity. India's existing legal architecture anchored by the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000 provides a foundational but demonstrably insufficient response to these evolving harms. This article undertakes a systematic doctrinal and analytical examination of the legislative framework governing digital child protection in India, identifies critical gaps in statutory coverage, enforcement capacity, and institutional coordination, and situates these findings within a comparative analysis of international instruments including the United Nations Convention on the Rights of the Child, the Budapest Convention on Cybercrime, and the United Kingdom's Online Safety Act, 2023. Drawing on judicial precedent, crime statistics from the National Crime Records Bureau, and scholarly literature, the study argues that India's present regulatory posture remains reactive and technologically unresponsive, failing to address emerging threats such as artificial intelligence generated abuse material, deep-fake exploitation, and dark-web trafficking networks.[1] The article advances a set of reform proposals encompassing legislative modernisation, capacity building

[1] Keywords: Digital Exploitation, Child Sexual Abuse Material, POCSO Act, Cybercrime, Online Safety, Legal Reform, India.

within law enforcement, mandatory platform accountability, and a child-centred digital literacy framework. It concludes that effective protection of children in the digital age demands a multi-stakeholder, proactive, and rights-based approach that aligns domestic law with global best practices.

I. INTRODUCTION

India stands at a critical juncture in its engagement with the digital world. Home to one of the largest and youngest online populations on earth, the country has witnessed extraordinary expansion in internet connectivity over the past decade. While this transformation has generated immense social and economic opportunity, it has simultaneously opened new avenues for the exploitation of children a group that is disproportionately exposed, under-equipped, and legally under-protected in digital environments.[2]

Online child exploitation is not a phenomenon confined to any single jurisdiction; it is a global challenge that demands coordinated legal and policy responses. In India, however, the legislative framework has struggled to keep pace with the velocity of technological change. Existing statutes most notably the Protection of Children from Sexual Offences Act, 2012 (POCSO) and the Information Technology Act, 2000 (IT Act) were conceived in an era that predates the emergence of encrypted messaging platforms, artificial intelligence–generated imagery, and the commodification of child abuse material on the dark web.[3]

Despite their foundational importance, these instruments leave substantial lacunae. The POCSO Act contains no express provisions addressing devices-mediated crimes beyond a limited treatment of child pornography, and the IT Act, while broader in its cybercrime mandate, does not address the specific vulnerabilities children face in digital spaces. The result is a fragmented and inconsistently enforced legal regime that fails to deter, detect, or adequately prosecute a wide spectrum of digital offences against minors.[4]

This article seeks to address that gap through a comprehensive legal analysis. It begins by establishing the nature and scale of the problem, proceeds through an examination of the applicable

[2] UNICEF, State of the World's Children Report (2021).
[3] Protection of Children from Sexual Offences Act, 2012 (India); Information Technology Act, 2000 (India).
[4] UNICEF India, Guidelines on Child Online Protection (2020).

Indian legal framework, undertakes a comparative review of international instruments, analyses representative judicial decisions and institutional responses, and concludes with a set of reform recommendations oriented toward a proactive, technologically adaptive, and child-centred legal architecture.

II. OBJECTS AND SCOPE OF STUDY

A. RESEARCH OBJECTIVES

This study pursues four interconnected objectives. First, it seeks to review and critically assess the existing legislative and policy framework governing the protection of children from online exploitation in India. Second, it aims to identify weaknesses and enforcement challenges that hinder effective child protection in digital environments. Third, it examines the roles of law enforcement agencies, internet service providers, and regulatory bodies in combating online exploitation. Fourth, it proposes concrete legal and policy reforms, drawing on comparative international experience, to strengthen India's digital child protection architecture.

B. SCOPE OF THE STUDY

The study encompasses the following dimensions: the nature and typology of digital exploitation, including online grooming, cyberbullying, CSAM, sextortion, trafficking, and artificial intelligence–facilitated exploitation; statutory analysis of the IT Act, 2000, the POCSO Act, 2012, the Juvenile Justice Act, 2015, and the Bharatiya Sakshya Adhiniyam, 2023; institutional analysis of the National Commission for Protection of Child Rights (NCPCR), the Indian Cyber Crime Coordination Centre (I4C), and state cybercrime cells; a comparative review of international instruments including the UNCRC, the Budapest Convention, and the UK Online Safety Act, 2023; and an examination of landmark judicial decisions shaping the field.[5]

The geographical scope is principally confined to India, although the comparative framework draws on international best practices and cross-border enforcement challenges as they bear upon domestic reform.

[5] Information Technology Act, 2000 (India); Protection of Children from Sexual Offences Act, 2012 (India); Digital Personal Data Protection Act, 2023 (India).

III. RESEARCH PROBLEM

India's legal and institutional framework for the protection of children from online exploitation is characterised by a fundamental misalignment between the pace of technological development and the adaptability of statutory responses. The POCSO Act and the IT Act, while representing legislative landmarks in their respective domains, were not designed to confront the full spectrum of digital threats that children encounter today. As a consequence, serious offences including AI-generated child abuse imagery, online grooming through encrypted platforms, and cross-border digital trafficking either fall outside the ambit of existing provisions or are addressed in terms that are insufficiently precise to ensure consistent prosecution.[67]

Beyond the substantive inadequacies of the statutory framework, enforcement presents equally acute difficulties. Many law enforcement agencies lack the technical expertise and digital forensic capacity necessary to investigate cybercrime offences effectively. Jurisdictional fragmentation a product of India's federal structure, which assigns law and order to state governments compounds the challenge, as cybercrime inherently transcends territorial boundaries. Institutional coordination between the NCPCR, the National Commission for Women, state cybercrime cells, and the I4C remains inconsistent, generating duplicated effort in some areas and dangerous gaps in others.

A further dimension of the problem is societal. The absence of widespread digital literacy among children, parents, and caregivers contributes to underreporting and leaves millions of potential victims without the awareness or tools to recognise and respond to exploitation. Social stigma associated with abuse discourages victims and families from engaging with law enforcement, further suppressing the reported incidence of offences and distorting the evidentiary record available to policymakers.[8]

These interlocking failures legislative, institutional, and social constitute the research problem that this study addresses.

[6] Cyberbullying Research Center, Annual Report on Digital Harassment (2022).
[7] International Labour Organization, Reports on Child Labour and Trafficking (2021).
[8] American Psychological Association, Report on Psychological Effects of Online Exploitation on Children (2020).

IV. RESEARCH QUESTIONS

This study is guided by the following research questions:

First, what are the principal legislative frameworks presently operative in India for the protection of children from online exploitation, and to what extent are they being effectively implemented?

Second, what are the major gaps and weaknesses in India's legal and institutional framework for protecting children from digital exploitation, and what structural factors account for those gaps?

Third, how do the roles of law enforcement agencies, internet service providers, and regulatory bodies influence the effectiveness of legal protections against online child exploitation?

Fourth, what legislative, institutional, and social reforms are most likely to strengthen India's capacity to protect children in digital environments, and how can those reforms draw on international best practice?

V. HYPOTHESIS

The central hypothesis of this study is that India's prevailing legal framework governing digital platforms remains structurally rigid and technologically inadequate in its capacity to address the rapidly evolving forms of digital exploitation of children. This inadequacy generates substantial regulatory and enforcement disparities that collectively impede efficient prevention, detection, and accountability across the full spectrum of online child exploitation. The study further hypothesises that targeted legislative reform, combined with institutional capacity building, mandatory platform accountability, and comprehensive digital literacy programs, would materially improve outcomes for child victims and reduce the incidence of digital exploitation. These hypotheses are tested through doctrinal analysis, comparative review, and examination of empirical evidence drawn from crime statistics and judicial decisions.

VI. METHODOLOGY

This study employs a doctrinal legal research methodology, supplemented by analytical and comparative approaches. The doctrinal dimension involves a systematic examination and interpretation of primary legal sources constitutional provisions, statutory enactments, delegated legislation, and judicial decisions to map the existing framework and identify its gaps. The analytical dimension draws on secondary academic literature, governmental reports, and empirical data to contextualise the legal analysis and assess the practical efficacy of existing provisions.

The comparative dimension situates the Indian framework within a global context by examining select international instruments and foreign legislative models. Jurisdictions selected for comparison principally the United Kingdom and relevant international treaty regimes were chosen because of both their institutional relevance to India's legal development and the sophistication of their contemporary digital child protection frameworks. Both deductive and inductive reasoning are employed: deductive reasoning draws on established legal principles to evaluate specific provisions, while inductive reasoning draws generalisable conclusions from the pattern of judicial decisions and institutional practice.

The study relies exclusively on pre-existing academic literature, government publications, judicial records, and statistical reports; it does not involve the collection of primary data from human subjects. All sources are cited in accordance with the Bluebook system of legal citation.

VII. LIMITATIONS OF THE STUDY

This study is subject to several limitations that bear acknowledgement. First, it relies exclusively on secondary data, including published reports, academic articles, and judicial records. This approach, while appropriate for doctrinal legal research, may fail to capture the full extent of unreported offences or the lived experience of victims, which are not systematically reflected in available documentary sources. Second, the rapid pace of technological development means that specific findings regarding particular digital platforms or exploitative techniques may become outdated as the technological environment evolves. Third, the extent of underreporting a function of social stigma, limited trust in law enforcement, and low digital awareness means that official crime statistics almost certainly understate the true prevalence of digital exploitation of children.

Fourth, the study's comparative dimension is necessarily selective; a more comprehensive global survey would require engagement with a wider range of jurisdictions. Fifth, the geographical focus on India, while appropriate to the study's primary aims, limits the transferability of findings to jurisdictions with different constitutional structures, enforcement capacities, or social contexts.

VIII. LITERATURE REVIEW

The scholarly literature on digital child exploitation in India spans legal analysis, criminological inquiry, and child protection policy. Five bodies of work are particularly salient to the present study.

A. LEGAL FRAMEWORK FOR ONLINE CHILD PORNOGRAPHY IN INDIA

Prior to the 2008 amendment to the Information Technology Act, India lacked specific legislation governing online child pornography, addressing the issue instead through general obscenity provisions of the Indian Penal Code, 1860. The enactment of Section 67B of the IT Act in 2009, following international pressure generated by India's ratification of the Optional Protocol to the Convention on the Rights of the Child, and the subsequent passage of the POCSO Act in 2012, established a more targeted legislative response. Scholarly commentary on these provisions observes that while the IT Act addresses the production, publication, and distribution of child pornography, and the POCSO Act criminalises the use of children in pornographic media, enforcement under both instruments remains weak. Reported cases under these provisions are few relative to the scale of the problem, and the intermediary liability framework which holds internet service providers to a strict liability standard subject to a due diligence defence has not generated the level of platform accountability that policymakers intended.

B. CYBERCRIME AND CHILD EXPLOITATION IN DIGITAL SPACES

A strand of the literature situates online child exploitation within the broader phenomenon of cybercrime, emphasising the distinctive challenges that digital offending poses for investigation and prosecution. This work observes that the use of false identities by offenders to groom children for offline meetings, the production of so-called 'made-to-order' abuse material, and the exploitation of gaming and messaging platforms as vectors for predatory contact have all intensified with advances in technology. The legal system's response, these scholars argue, is

constrained both by the inadequacy of existing substantive provisions and by the practical limitations of law enforcement particularly the absence of specialised training, insufficient digital forensic capacity, and the inherent difficulty of apprehending criminals who deploy encryption, anonymisation tools, and transnational digital infrastructure.[9]

C. CHILD PROTECTION POLICY: INSTITUTIONAL GAPS AND NORMATIVE DEFICITS

Research on child protection policy in India identifies a persistent gap between legislative aspiration and implementation reality. Despite a substantial body of protective legislation including the Juvenile Justice (Care and Protection of Children) Act, the POCSO Act, and the CHILDLINE initiative annual mortality and abuse statistics confirm that millions of Indian children remain unprotected in practice. Scholars identify two intersecting causes: a normative deficit arising from the failure to incorporate digital forms of exploitation into child protection frameworks, and an institutional deficit manifested in the absence of adequate awareness among the general public about the scope of protective legislation and the mechanisms available for reporting abuse. This literature emphasises that legal literacy and community engagement are prerequisites for the effective functioning of any child protection system.[10]

D. CONSTITUTIONAL AND SYSTEMIC CHALLENGES TO CHILD RIGHTS

A body of work focused on constitutional and institutional dimensions of child rights protection in India examines the structural obstacles to the effective enforcement of protective legislation. This scholarship identifies the fragmentation of institutional responsibility across national commissions, state-level agencies, and civil society bodies as a primary source of inefficiency. While entities such as the NCPCR and the NCW carry significant advisory and monitoring mandates, neither possesses direct investigative or prosecutorial powers, leaving enforcement dependent on police forces that are frequently underfunded and inadequately trained. The literature further notes that grassroots organisations play a critical but undervalued role in bridging the gap between formal legal frameworks and the communities most in need of protection.

E. DIGITAL SAFETY, ONLINE ABUSE, AND ACCESS TO JUSTICE

[9] NSPCC (UK), Child Protection Online Safety Reports (2021).
[10] UN Committee on the Rights of the Child, General Comment on Children's Rights in the Digital Environment (2021).

Empirical research on the digital safety of Indian children highlights a stark disparity between rapidly increasing internet access and the persistence of offline risk factors poverty, gender discrimination, inadequate education that amplify children's vulnerability online. Scholars in this field note that while universal primary school enrolment has been achieved, dropout rates increase sharply as students advance through the educational system, particularly among marginalised groups, leaving a significant proportion of the child population without the protective benefits of sustained formal education. The emergence of cyberbullying, online harassment, and exposure to sexualised content as significant risks for the millions of Indian children who now access the internet via smartphones is identified as an area requiring urgent legislative and programmatic attention. This literature underscores the need for updated regulatory frameworks and adequately resourced child protection services capable of responding to the particular vulnerabilities of the digital age.

IX. CONCLUSION AND REFORM RECOMMENDATIONS

The foregoing analysis confirms the hypothesis with which this study began. India's legal framework for the protection of children from digital exploitation, while foundationally significant, is structurally inadequate to address the contemporary landscape of online harm. The POCSO Act and the IT Act remain the twin pillars of the system, but both instruments exhibit the limitations of statutes conceived before the maturation of mobile internet, encrypted communications, and generative artificial intelligence. The result is a protective framework that is reactive in orientation, fragmented in its institutional architecture, and under-resourced in its enforcement capacity.[11][12]

The comparative analysis of international frameworks identifies several reform vectors of direct relevance to India. The UK's Online Safety Act, 2023, with its proactive duty of care imposed on online platforms, its mandatory child safety risk assessment regime, and its provision for substantial financial penalties for non-compliance, represents a model of platform accountability that India has yet to adopt. The Budapest Convention's framework for international

[11] National Crime Records Bureau; National Cyber Crime Reporting Portal, CCPWC Statistics and NCMEC Tip-Line Data (2019–2024).
[12] Analysis of Legal and Systemic Challenges in India with Reference to the Protection of Children from Sexual Offences Act, 2012 and Information Technology Act, 2000.

cooperation in cybercrime investigation and evidence gathering addresses the jurisdictional fragmentation that currently hampers cross-border enforcement. The Lanzarote Convention's victim-centred substantive approach, criminalising a broader range of predatory conduct including grooming and intentional access to abuse material, fills gaps that the POCSO Act leaves unaddressed.

On the basis of this analysis, the following reform recommendations are advanced. First, India should enact a dedicated Online Child Safety Act that imposes clear duties of care on digital platforms, mandates child safety risk assessments, and establishes proportionate enforcement mechanisms including financial penalties and, in egregious cases, platform access restrictions. Second, the POCSO Act and the IT Act should be amended to expressly address AI-generated CSAM, online grooming as a standalone offence, and the use of encrypted platforms and the dark web in the commission of child exploitation offences. Third, the institutional architecture for digital child protection should be rationalised, with clear lines of authority between the NCPCR, the I4C, and state cybercrime cells, supported by adequate resources and standardised protocols. Fourth, India should engage constructively with the international cybercrime treaty framework, either through accession to the Budapest Convention or through bilateral information-sharing agreements that achieve equivalent outcomes. Fifth, a comprehensive national digital literacy program targeted at children, parents, and educators should be developed and funded as a matter of priority, recognising that legal reform without accompanying social awareness cannot effectively reduce exploitation.[13][14]

Protecting children in the digital age is simultaneously a legal obligation, a policy imperative, and a moral commitment. India possesses the institutional foundation, the constitutional commitment to child welfare, and the technological capacity to build a world-class digital child protection system. What is required is the political will to update the legal framework, invest in enforcement capacity, and place the rights and safety of children at the centre of its engagement with the digital economy. Achieving that outcome is the overriding objective that this study has sought to advance.

[13] National Crime Records Bureau, Crime in India Reports (2019–2023); Studies on Cybercrime Investigation Challenges in India.
[14] Ministry of Home Affairs, Government of India, Cybercrime Prevention Initiatives; Policy Recommendations on Capacity Building (2022).