



KAMARAJ IAS ACADEMY
Only IAS Academy by Grandson of "Perunthalsivam Kamarajar"

Online Child Sexual Exploitation and Abuse Material Raises Concerns Over Platform Accountability and Child Safety in India

Published On: 16-09-2026

Recent Developments:

- In **July 2026**, the Government took serious note of reports alleging advertisements linked to **Child Sexual Exploitative and Abuse Material (CSEAM)** on social media platforms and sought a detailed report from the concerned intermediary. The **National Commission for Protection of Child Rights (NCPCR)** also issued notice to the concerned platforms.
- In **September 2026**, the NCPCR summoned senior Meta India executives in connection with advertisements allegedly linked to CSEAM on Meta-owned platforms and instituted an inquiry to establish the facts and examine the platform's role.
- The episode has highlighted concerns regarding **algorithmic moderation, advertising systems, platform due diligence, monetisation of harmful content and intermediary accountability**, rather than only the conduct of individual users.
- The Government has also strengthened the **Information Technology Rules, 2021** through amendments effective from **20 February 2026**, including safeguards addressing synthetically generated information such as deepfakes and CSEAM. The prescribed response period for certain reported intimate or sexually explicit content has also been reduced from 24 hours to **2 hours**.

Why Does CSEAM Reach Social Media Platforms?

Limitations of Automated Moderation:

- Automated safety systems generally depend on **content matching, classifiers, metadata and previously identified harmful material**, which can be challenged by manipulated images, coded language, altered media and rapidly changing evasion techniques.
- Artificial intelligence systems may therefore produce **false negatives**, particularly when harmful material is disguised or distributed through indirect forms rather than uploaded in an immediately recognisable form.

Misclassification and Moderation Gaps:

- Harmful material may be incorrectly classified as generic adult or sexually explicit content, potentially preventing the application of stronger **child-safety safeguards**.
- Dependence on automated systems without adequate human review can create gaps in detection, escalation and removal, particularly when platforms process extremely large volumes of content.

Advertising and Monetisation Risks:

- The issue is especially significant when illegal material is promoted through **paid advertising or recommendation systems**, because platform systems may contribute to the visibility, targeting or monetisation of harmful content.

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

- The regulatory question therefore extends beyond content hosting to the broader responsibility of platforms for **selection, amplification and commercial distribution** of unlawful material.

Indirect or Bait-Based Distribution:

- CSEAM-related advertisements may use indirect references, external links, usernames or other mechanisms to redirect users towards closed or encrypted communication spaces where unlawful material may be distributed.
- Such tactics create an enforcement challenge because the initial advertisement may not itself contain the complete illegal material, while still functioning as a gateway to its distribution.

Human Moderation Challenges:

- Human reviewers may face **high workloads, limited contextual information and rapidly evolving forms of abuse**, increasing the possibility of erroneous decisions.
- Effective moderation therefore requires a combination of automated detection, trained human review, rapid escalation, evidence preservation and cooperation with law-enforcement agencies.

Legal and Regulatory Framework in India:

Protection of Children from Sexual Offences Act, 2012:

- The **Protection of Children from Sexual Offences Act, 2012 (POCSO Act)** provides a comprehensive framework for protecting children below 18 years from sexual offences, including offences involving the use of children for pornographic purposes.
- **Section 13** deals with the use of a child for pornographic purposes, while **Section 14** prescribes punishment for such use.
- **Section 15** specifically addresses the storage or possession of pornographic material involving a child, including circumstances involving transmission, propagation, display, distribution or commercial purpose.
- **Section 19** establishes the reporting of offences, while Section 21 provides punishment for failure to report or record a case.

Information Technology Act, 2000:

- **Section 67B** specifically deals with publishing, transmitting or facilitating material depicting children in sexually explicit acts in electronic form and provides criminal punishment for such conduct.
- **Section 79** provides conditional safe-harbour protection to intermediaries for third-party information, subject to compliance with statutory and regulatory requirements, including applicable due-diligence obligations.
- The legal framework therefore balances intermediary protection with accountability when platforms fail to comply with prescribed obligations or facilitate unlawful activity.

Information Technology Rules, 2021:

- The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** impose due-diligence obligations on intermediaries and require significant social media intermediaries to make reasonable efforts to deploy appropriate technical measures, including **automated tools**, to proactively identify certain harmful material involving rape and child sexual abuse or exploitation.
- The Rules also establish institutional compliance requirements for significant social media intermediaries, including designated compliance and grievance-redressal mechanisms.
- The 2026 amendments strengthened safeguards relating to **synthetically generated information, deepfakes, CSEAM and non-consensual intimate imagery**, reflecting the changing nature of technology-enabled child exploitation.

Digital Personal Data Protection Act, 2023:

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

- The **Digital Personal Data Protection Act, 2023** provides specific safeguards concerning children's personal data and restricts behavioural monitoring and targeted advertising directed at children, subject to the statutory framework.
- This creates an additional layer of protection by linking **child safety, privacy and responsible digital-platform practices**.

Government Mechanisms to Combat Online Child Exploitation:

National Cyber Crime Reporting Portal:

- The **National Cyber Crime Reporting Portal** enables citizens to report cybercrime, including online CSEAM and sexually explicit content involving children, and provides facilities for anonymous reporting in relevant categories.
- Complaints are handled by the concerned **State and Union Territory law-enforcement agencies**, which undertake investigation, registration of cases and further legal action.

Indian Cyber Crime Coordination Centre:

- The **Indian Cyber Crime Coordination Centre (I4C)** provides an institutional framework for coordinated action against cybercrime, including crimes targeting women and children.
- The Government has also supported cyber-forensic laboratories, capacity building and training of law-enforcement personnel, prosecutors and judicial officers under the **Cyber Crime Prevention against Women and Children Scheme**.

Cooperation with International Organisations:

- The **National Crime Records Bureau (NCRB)** has an arrangement with the **National Center for Missing and Exploited Children (NCMEC), United States**, for sharing relevant cyber-tipline reports concerning online child sexual exploitation with Indian States and Union Territories for further action.
- NCRB has also been designated as a Government agency authorised to issue notices to intermediaries under Section 79(3)(b) of the Information Technology Act for specified unlawful child sexual exploitation and related content.

National Commission for Protection of Child Rights:

Statutory Status and Composition:

- The **National Commission for Protection of Child Rights (NCPCR)** is a statutory body constituted under Section 3 of the **Commissions for Protection of Child Rights Act, 2005** and functions under the administrative control of the Ministry of Women and Child Development.
- It was established in **March 2007** to protect, promote and defend child rights and to monitor the implementation of important child-related laws, including the POCSO Act and the Right of Children to Free and Compulsory Education Act, 2009.
- The Commission consists of a **Chairperson and 6 members**, of whom at least 2 must be women, with members selected from fields including education, child health, child development, juvenile justice, child labour, child psychology and laws relating to children.

Functions and Powers:

- NCPCR examines safeguards for child rights, inquires into violations, reviews policies and laws, undertakes research, promotes child-rights awareness and can take **suo motu cognisance** of matters involving deprivation or violation of child rights.
- While conducting inquiries, the Commission possesses specified powers of a **civil court**, including summoning persons, examining them on oath, requiring production of documents and requisitioning public

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

records.

- Following an inquiry, NCPCR may recommend prosecution or other action to the concerned Government or authority and may approach the **Supreme Court or High Court** for appropriate directions, orders or writs.
- Its role is primarily **investigative, recommendatory and supervisory**; it does not function as a regular criminal court and does not itself impose criminal punishment.

International and Constitutional Dimensions:

Convention on the Rights of the Child:

- The **United Nations Convention on the Rights of the Child, 1989** establishes internationally recognised civil, political, economic, social and cultural rights of children.
- India ratified the Convention in **1992**, thereby strengthening its international commitment to protecting children from exploitation, abuse and other violations.
- The Convention provides an important normative foundation for India's child-protection framework and complements domestic legislation such as the POCSO Act and the Commissions for Protection of Child Rights Act.

Constitutional Framework:

- Child protection is supported by several constitutional provisions, including **Article 15(3)**, which permits special provisions for children, **Article 21**, which protects life and personal liberty, and **Article 39(e) and 39(f)**, which direct the State to protect children from exploitation and ensure healthy development in conditions of freedom and dignity.
- These provisions establish child protection as both a **fundamental rights concern and a directive principle of governance**.

Challenges and Way Forward:

Strengthening Platform Accountability:

- Platforms should adopt **risk-based content governance**, independent audits, transparent advertising review systems and stronger safeguards against algorithmic amplification of harmful material.
- Automated detection should be combined with trained human moderation, specialist child-safety teams and rapid escalation channels for suspected CSEAM.
- Greater transparency is required regarding how advertising, recommendation and monetisation systems interact with harmful content.

Improving Institutional Coordination:

- **NCPCR, MeitY, MHA, I4C, NCRB, State police and digital platforms** should maintain interoperable reporting and response mechanisms for rapid identification, removal and investigation.
- The Parliamentary Standing Committee has also highlighted the need to strengthen NCPCR's manpower, resources and digital coordination mechanisms, including integration of its child-protection portals for more effective monitoring.

Protecting Children Without Undermining Digital Rights:

- Regulation must combine **child safety, privacy, freedom of expression, procedural safeguards and technological innovation**, rather than relying solely on blanket content removal.
- Stronger international cooperation is necessary because online child exploitation frequently crosses national jurisdictions and involves platforms, payment systems and encrypted communication services located in different countries.

Value Addition for UPSC:

Mains Enrichment:

- **Constitutional linkage:** Articles 15(3), 21, 39(e) and 39(f).
- **Legal linkage:** POCSO Act, 2012; Information Technology Act, 2000; Information Technology Rules, 2021; Digital Personal Data Protection Act, 2023.
- **Institutional linkage:** NCPCR, I4C, NCRB, MeitY and State law-enforcement agencies.
- **Way forward:** India needs a **rights-based, technology-enabled and institutionally coordinated child-safety architecture** that makes digital platforms accountable while preserving legitimate digital freedoms.