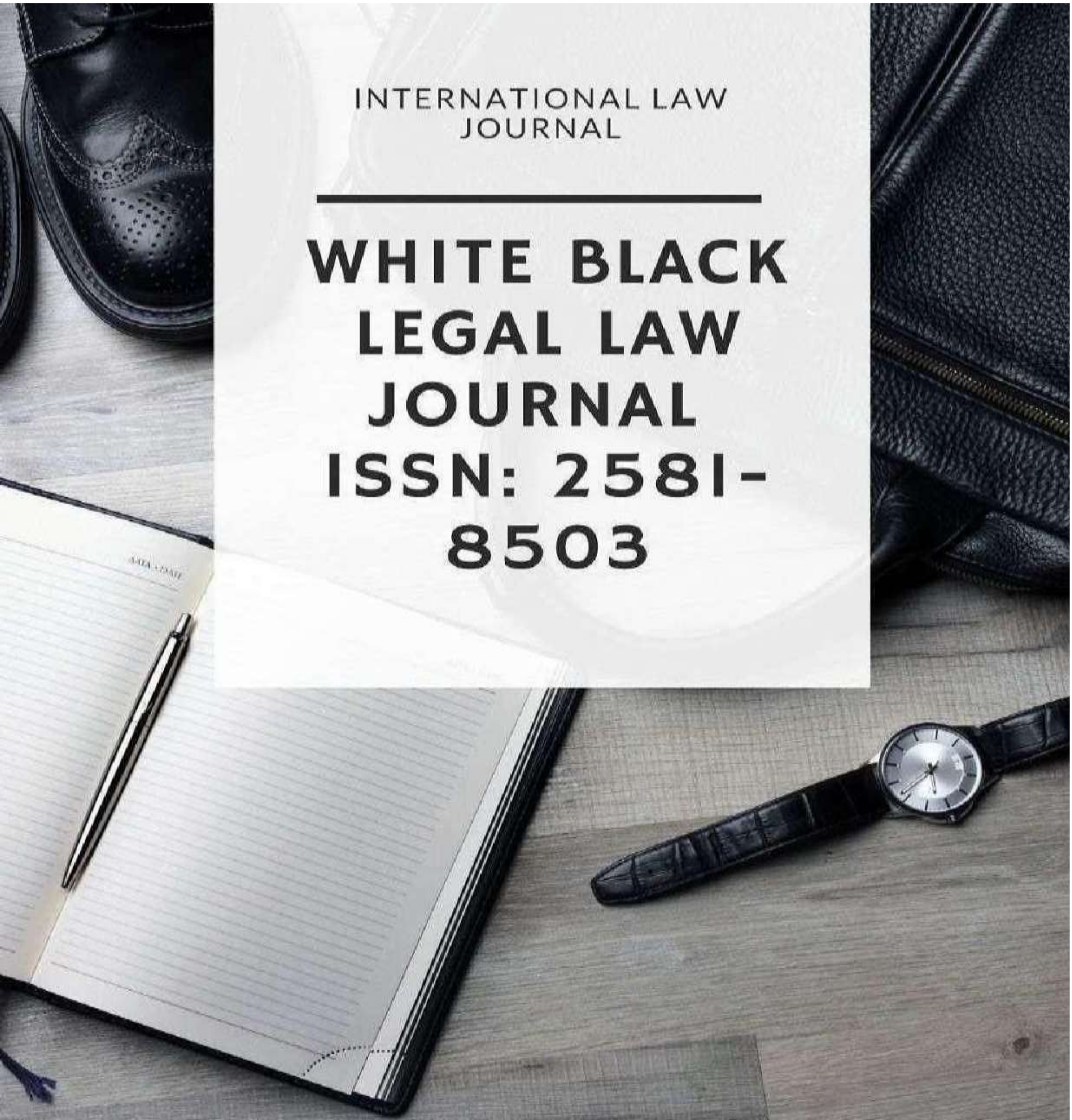

INTERNATIONAL LAW JOURNAL

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 or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

THE ROLE OF LAW ENFORCEMENT IN PREVENTING ONLINE CRIMES AGAINST CHILDREN

AUTHORED BY - MS UPASANA SHARMA[1] & DR. MITHLESH BANSAL[2]

Introduction

The rapid proliferation of digital technologies has transformed the landscape of childhood, offering unprecedented opportunities for learning, socialisation, and creativity. However, this digital revolution has also exposed children to a spectrum of online threats, including sexual exploitation, grooming, cyberbullying, trafficking, and exposure to harmful content. Law enforcement agencies worldwide are at the forefront of efforts to prevent, detect, and respond to these crimes. Their role is multifaceted, encompassing legal enforcement, technological innovation, inter-agency coordination, victim support, and international collaboration. This research scheme provides a comprehensive, structured plan to investigate the role of law enforcement in preventing online crimes against children, with a focus on legal frameworks, investigative techniques, institutional arrangements, technology use, challenges, and best practices across jurisdictions.

1. Overview: The Role of Law Enforcement in Preventing Online Crimes Against Children

Law enforcement agencies are pivotal in the fight against online crimes targeting children. Their responsibilities span from proactive prevention and public education to the investigation and prosecution of offenders. The complexity of online child exploitation, characterised by anonymity, global reach, and rapidly evolving technologies, demands a holistic, multi-sectoral response. Law enforcement must not only enforce laws but also collaborate with technology companies, educators, social services, and international partners to create a safer digital environment for children.

The scope of online crimes against children includes, but is not limited to:

- Child sexual abuse material (CSAM) production, distribution, and possession
- Online grooming and enticement

[1] Research Scholar, Faculty of Law, Tantia University, Sri Ganganagar.

[2] Assistant Professor of Law, Faculty of Law, Tantia University, Sri Ganganagar.

- Cyberbullying and harassment
- Sextortion and identity theft
- Trafficking and exploitation via digital platforms

The effectiveness of law enforcement is contingent upon robust legal frameworks, specialised training, technological capacity, inter-agency and international cooperation, and child-sensitive procedures.[3][4]

2. Legal Frameworks

2.1 International Instruments and Standards

International legal instruments provide the foundation for national laws and cross-border cooperation in combating online crimes against children. Key instruments include:

- **United Nations Convention on the Rights of the Child (UNCRC)**: Mandates the protection of children from all forms of exploitation, including online abuse.
- **Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (OPSC)**: Requires states to criminalise the sale of children, child prostitution, and child pornography, and to provide for international cooperation in investigation and prosecution.[5] [6]
- **ILO Convention No. 182**: Prohibits the worst forms of child labour, including the use of children in pornography.
- **Budapest Convention on Cybercrime**: The first international treaty seeking to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations.[7] [8]
- **WeProtect Global Alliance Model National Response**: Provides a comprehensive framework for national strategies, emphasising legislation, prevention, law enforcement training, industry collaboration, data collection, and victim support.[9] [10]

[3] Available at https://ijoss.in/wp-content/uploads/2025/03/1.-_Cyber-Crimes-Against-Children_-Legal-Challenges-and-Rights-Protection._.pdf.

[4] Available at https://www.unicef.org/media/169261/file/Multidisciplinary%20Models%20of%20Care.pdf

[5] Available at https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child

[6] Available at https://www.unicef.org/child-rights-convention/strengthening-convention-optional-protocols

[7] Available at https://legalresearchandanalysis.com/wp-content/uploads/2025/03/CYBERCRIMEINCROSS-BORDERJURISDICTIONS-pdf.pdf

[8] Available at https://ijirl.com/wp-content/uploads/2025/03/ADJUDICATING-AND-INVESTIGATING-CROSS-BORDER-CYBERCRIMES-A-STUDY-OF-INDIAS-JURISDICTIONAL-FRAMEWORK.pdf

[9] Available at https://www.weprotect.org/resources/frameworks/model-national-response/

[10] Available at https://www.safefutureshub.org/solutions/weprotect-model-national-response

- **ITU Guidelines on Child Online Protection**: Offers policy and technical guidance for governments, industry, and educators.[11]

These instruments set minimum standards for criminalisation, victim protection, and international cooperation, and are reflected in national laws and policies.

Table 1: Key International Instruments

Instrument	Scope and Requirements	Adoption Status (India)
UNCRC	Broad child rights, including protection from exploitation	Ratified
OPSC	Criminalisation of sale, prostitution, pornography; international cooperation	Ratified
ILO Convention No. 182	Prohibits the worst forms of child labour, including pornography	Ratified
Budapest Convention on Cybercrime	Harmonisation of cybercrime laws, cooperation, and evidence sharing	Not signed
WeProtect Global Alliance Model National Response	Comprehensive national response framework	Referenced
ITU Guidelines on Child Online Protection	Policy and technical guidance	Referenced

International standards guide the development of national legal frameworks and facilitate cross-border collaboration, which is essential given the transnational nature of online child exploitation.

2.2 Legal Frameworks — India (National Laws and Policies)

India has developed a multi-layered legal framework to address online crimes against children, drawing from both international obligations and domestic realities. The principal statutes include:

- **Protection of Children from Sexual Offences (POCSO) Act, 2012**: Criminalises a wide range of sexual offences against children, including those committed online. The 2019 amendment introduced Section 15, which specifically penalises the possession,

[11] Available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx

storage, and viewing of child sexual abuse material (CSEAM), even without intent to distribute, following a landmark Supreme Court judgment in 2024. [12]

- **Information Technology (IT) Act, 2000 (as amended)**: Section 67B criminalises the publication, transmission, and even browsing or downloading of child sexual abuse material in electronic form. The law also imposes obligations on intermediaries (e.g., social media platforms) to remove such content and cooperate with law enforcement.[13]
- **Juvenile Justice (Care and Protection of Children) Act, 2015**: Provides for the care, protection, and rehabilitation of children in conflict with the law or in need of care, emphasising child-friendly procedures.
- **Indian Penal Code (IPC)/Bharatiya Nyaya Sanhita (BNS), 2023**: Contains provisions on trafficking, sexual exploitation, and related offences.
- **Digital Personal Data Protection (DPDP) Act, 2023**: Regulates the processing of digital personal data, including that of children, and mandates safeguards for their privacy.[14]
- **Intermediary Guidelines and Digital Media Ethics Code (IT Rules), 2021**: Mandate social media and digital platforms to proactively remove harmful content related to children and comply with government directives.

Table 2: Key Indian Legal Provisions

Law/Provision	**Scope and Key Features**
POCSO Act, 2012 (as amended)	Criminalises sexual offences against children, including online; Section 15 covers CSEAM possession
IT Act, 2000 (Section 67B)	Criminalises publication, transmission, browsing, and downloading of CSAM; intermediary obligations
JJ Act, 2015	Child-friendly procedures, care and protection, rehabilitation
IPC/BNS	Trafficking, sexual exploitation, abduction, and related offences
DPDP Act, 2023	Data protection, privacy safeguards for children
IT Rules, 2021	Platform obligations for content removal, reporting, and user safety

Despite these robust laws, enforcement challenges persist, including gaps in addressing

[12] Available at https://www.barandbench.com/view-point/supreme-court-landmark-ruling-child-pornography-legal-shift-gaps-policies

[13] Available at https://www.apnilaw.com/legal-articles/acts/punishment-under-section-67b-it-act-pocso-act-overlap/

[14] Available at https://penacclaims.com/wp-content/uploads/2025/05/Yashwant-Soni.pdf

emerging threats (e.g., deepfakes, AI-generated CSAM), resource constraints, and jurisdictional complexities.

2.3 Comparative Legal Frameworks — Selected Jurisdictions

A comparative analysis of legal frameworks in the US, UK, EU, Australia, and Brazil reveals both convergence and divergence in approaches to online child protection.

Table 3: Comparative Legal Frameworks

Aspect	India	USA	EU/UK	Australia	Brazil
Primary Law	IT Act, POCSO Act	PROTECT Act, COPPA, Child Pornography Act	GDPR, Sexual Offences Act, Online Safety Act	Criminal Code Act, Enhancing Online Safety	Child and Adolescent Statute
Definition of Child	Below 18 (POCSO)	Below 13 (COPPA), below 18 (others)	Below 16 (GDPR), below 18 (others)	Below 18	Below 18
Grooming Laws	POCSO, IT Act	PROTECT Act, federal/state laws	EU Directive 2011/93/EU, Sexual Offences Act	Criminal Code (Sections 474.26, 474.27)	Child and Adolescent Statute
CSAM/Online Exploitation	POCSO, IT Act	Child Pornography Prevention Act, PROTECT	Strictly prohibited, GDPR	Prohibited, eSafety Commissioner	Prohibited
Data Protection	DPDP Act, IT Rules	COPPA, state laws	GDPR, UK GDPR	Privacy Act	Data Protection Law

Platform Obligations	IT Rules, Sahyog Portal	NCMEC reporting, COPPA	Online Safety Act, DSA, IWF, CEOP	eSafety Commissioner	SaferNet, OAS
Reporting Mechanisms	Cybercrime Portal, Childline 1098	CyberTipline (NCMEC), FBI IC3	EUROPOL, INHOPE, IWF, CEOP	eSafety Commissioner, reporting tool	SaferNet, national hotlines
Penalties	Up to life imprisonment, heavy fines	Up to 30 years, heavy fines	Strict GDPR penalties, up to life imprisonment	Up to 25 years, heavy fines	Up to 20 years, fines

Key Observations:

- The US and UK have specialised agencies (e.g., NCMEC, CEOP) and strong reporting mechanisms.
- The EU emphasises data protection and platform accountability (GDPR, DSA).
- Australia's eSafety Commissioner is a global leader in online child safety enforcement.
- Brazil's SaferNet and Federal Police play central roles in enforcement and victim support.
- India's framework is comprehensive but faces enforcement and capacity challenges, especially in cross-border cases.

3. Enforcement Models and Institutional Arrangements

3.1 Specialised Law Enforcement Units

Effective prevention and investigation of online crimes against children requires specialised units with dedicated resources and expertise. Models include:

- **Cybercrime Units**: National and state-level units focusing on cyber-enabled crimes, including CSAM, grooming, and trafficking.
- **Victim Identification Task Forces**: Multidisciplinary teams (e.g., Europol's VIDTF, INTERPOL's Crimes Against Children unit) that analyse digital evidence to identify and rescue victims.[15]

[15] Available at https://www.interpol.int/en/News-and-Events/News/2025/20-arrested-in-international-operation-targeting-child-sexual-abuse-material

- **Children's Advocacy Centres (CACs)** and Barnahus Models: Multidisciplinary, child-friendly centres that coordinate law enforcement, child protection, medical, and psychological services to minimise trauma and improve outcomes.
- **One Stop Centres (OSCs) and Family Justice Centres (FJCs)**: Co-located services for victims, integrating legal, medical, and psychosocial support.

Table 4: Enforcement Models Across Jurisdictions

Country/Region	**Specialised Units/Models**	**Key Features**
India	Cybercrime Units, I4C, CyTrain, Sahyog	National/state units, training, reporting portals
USA	FBI, ICE, NCMEC, ICAC Task Forces	Federal/state task forces, victim-centred approach
UK	National Crime Agency, CEOP, CACs	Multidisciplinary, child-friendly, strong victim support
EU	Europol EC3, Barnahus, CACs	Multinational task forces, forensic analysis, and victim ID
Australia	AFP, eSafety Commissioner, OSCs	Specialised cybercrime units, online safety regulation
Brazil	Federal Police, SaferNet	National cybercrime units, hotline, victim support

Analysis:

Specialised units and multidisciplinary models (e.g., CACs, Barnahus) are associated with higher rates of victim identification, better child outcomes, and more effective prosecutions. India's I4C, CyTrain, and Sahyog Portal represent significant progress but require further investment and integration with child protection and social services.

4. International Cooperation and Mutual Legal Assistance

4.1 Mechanisms for Cross-Border Collaboration

Given the global nature of online child exploitation, international cooperation is essential. Mechanisms include:

- **Mutual Legal Assistance Treaties (MLATs):** Bilateral/multilateral treaties for evidence sharing, extradition, and joint investigations. India has MLATs with 42 countries but faces delays and bureaucratic hurdles.

- **INTERPOL and Europol**: Facilitate information exchange, joint operations, and victim identification task forces (e.g., Europol's VIDTF, INTERPOL's Crimes Against Children unit).[16]
- **G8 24/7 Network**: Rapid response network for urgent data preservation and investigative assistance.
- **INHOPE and NCMEC**: Global networks of hotlines and clearinghouses for reporting, triage, and referral of CSAM cases.

Table 5: International Cooperation Mechanisms

Mechanism	Functionality	India's Participation
MLATs	Evidence sharing, extradition, joint ops	Yes (42 countries)
INTERPOL/Europol	Information exchange, joint task forces	Yes
G8 24/7 Network	Rapid data preservation, urgent assistance	Yes
INHOPE/NCMEC	Hotline network, CSAM reporting	Yes (via MoU)
Budapest Convention	Harmonisation, expedited cooperation	No

Challenges:

India's non-signatory status to the Budapest Convention limits access to streamlined cooperation and expedited evidence sharing. MLAT processes are often slow (6–24 months), hampering timely investigations.

4.2 Case Studies: International Operations

- **Operation Vibora (2024–2025)**: Spanish National Police, INTERPOL, and Europol coordinated to arrest 20 suspects across 12 countries, identify 68 additional suspects, and seize digital evidence, demonstrating the power of international task forces.
- **Europol VIDTF (2025)**: 51 children identified and safeguarded, 213 leads sent to national authorities, highlighting the impact of multinational victim identification efforts.

[16] Available at https://legalresearchandanalysis.com/wp-content/uploads/2025/03/CYBERCRIMEINCROSS-BORDERJURISDICTIONS-pdf.pdf

5. Public-Private Partnerships and Platform Responsibilities

5.1 Platform Obligations and Safety-by-Design

- **Legal Obligations**: Laws such as India's IT Rules, the UK's Online Safety Act, and the EU's Digital Services Act impose duties on platforms to detect, remove, and report CSAM, implement age verification, and provide user safety features.[17]
- **Automated Detection and Takedown**: Platforms use AI tools (e.g., PhotoDNA, hash matching) to proactively detect and remove CSAM, often in partnership with law enforcement and NGOs.
- **Reporting Mechanisms**: Platforms must provide accessible reporting tools for users and cooperate with law enforcement for evidence sharing and investigations.

5.2 Public-Private Collaboration

- **Sahyog Portal (India)**: Centralized platform for real-time takedown requests and coordination between government agencies and social media intermediaries. Platforms are required to nominate nodal officers, develop APIs for integration, and submit periodic compliance reports.
- **Industry Initiatives**: Tech companies (e.g., Microsoft, Meta, Google) collaborate with NGOs (e.g., Thorn, IWF) and law enforcement to develop detection tools, share best practices, and run awareness campaigns.

Challenges:

Jurisdictional conflicts, privacy laws, and differing legal obligations across countries complicate platform compliance. Resistance from global tech companies over dual reporting requirements (e.g., NCMEC vs. Sahyog) highlights the need for harmonized standards and international agreements.

6. Victim Identification, Support, and Child-Sensitive Procedures

6.1 Victim Identification

- **Victim-Centred Investigations: Prioritise** the identification and rescue of victims depicted in CSAM, using image analysis, facial recognition, and international databases (e.g., NCMEC CVIP, INTERPOL, Europol).

[17] Available at https://www.gov.uk/government/publications/online-safety-act-protection-of-children-codes-of-practice-explanatory-memorandum/online-safety-act-protection-of-children-codes-of-practice-explanatory-memorandum

- **Specialized Task Forces**: Multinational teams collaborate to analyze evidence, share leads, and coordinate rescues.

6.2 Child-Sensitive Procedures

- **Forensic Interviews and Testimony**: Conducted in child-friendly environments by trained professionals to minimize trauma and ensure reliable evidence.
- **Legal Safeguards**: In-camera trials, protection of identity, and support for child witnesses as mandated by POCSO and international protocols.
- **Psychosocial Support**: Access to counseling, therapy, and rehabilitation services for victims and families.

7. Prevention, Education, and Community Awareness

7.1 Digital Literacy and Online Safety Education

- **School-Based Programs**: Integration of digital safety, cyberbullying prevention, and responsible technology use into curricula (e.g., ChildFund India, SG Cyber Safe Students Programme, CBSE guidelines).[18]
- **Teacher and Parent Training**: Empower educators and caregivers to recognize signs of exploitation and support children in safe online practices.
- **Peer Education and Youth Leadership**: Programs that train youth leaders to educate peers and promote digital safety.

7.2 Public Awareness Campaigns

- **Government and NGO Initiatives**: Nationwide campaigns to raise awareness of online risks, reporting mechanisms, and available support services.
- **Community Partnerships**: Engagement with local organizations, law enforcement, and child protection units to strengthen prevention and response networks.

8. Ethical, Privacy, and Human Rights Considerations

8.1 Balancing Protection and Privacy

- **Data Protection Laws:** Compliance with national and international data protection standards (e.g., DPDP Act, GDPR) to safeguard children's privacy while enabling

[18] Available at https://www.csa.gov.sg/our-programmes/cybersecurity-outreach/sg-cyber-safe-students/

effective investigations.[19]

- **Ethical Use of AI and Surveillance**: Transparency, accountability, and oversight in the deployment of AI tools for detection and investigation, with safeguards against bias and misuse.
- **Child Participation and Autonomy**: Respect for children's rights to privacy, participation, and protection in all interventions and policy decisions.

8.2 Addressing the Digital Divide

- **Equitable Access**: Ensuring that children from disadvantaged backgrounds have access to digital safety tools and education, and are not disproportionately exposed to online risks.

9. Policy Recommendations and Reform Options

9.1 Legislative Reforms

- **Update and Harmonise Laws: Amend existing laws to address emerging threats (e.g., deepfakes, AI-generated CSAM), clarify platform obligations, and harmonise** with international standards (e.g., Budapest Convention).[20]
- **Standalone Digital Child Protection Statute**: Enact comprehensive legislation covering all aspects of online child exploitation, platform liability, and children's digital rights.

9.2 Institutional and Capacity Building

- **Expand Specialized Units**: Increase investment in cybercrime units, victim identification task forces, and multidisciplinary centers.
- **Continuous Training**: Mandate ongoing, scenario-based training for law enforcement, judiciary, educators, and social workers.

9.3 Technology and Innovation

- **AI and Automation**: Invest in AI-driven detection, grooming prevention, and evidence management tools, with ethical oversight.

[19] Available at https://www.guardii.ai/blog/how-ai-detects-grooming-behavior-online

[20] Available at https://iircj.org/wp-content/uploads/15.-Strengthening-Indias-Cybercrime-Response-A-Gender-and-Child-Centric-Legal-and-Institutional-Framework.pdf

- **Safety-by-Design Regulation**: Require platforms to embed safety features, conduct risk assessments, and cooperate with law enforcement.

9.4 International Cooperation

- **Ratify the Budapest Convention**: Streamline cross-border evidence sharing and cooperation.
- **Strengthen MLAT Processes**: Develop expedited bilateral agreements and participate in global networks (e.g., G8 24/7).

9.5 Prevention and Education

- **Integrate Digital Literacy**: Make online safety education mandatory in schools, with resources for teachers, parents, and youth leaders.
- **Community Engagement**: Support peer education, youth leadership, and community-based prevention initiatives.

9.6 Victim Support and Child-Sensitive Procedures

- **Mandate Child-Friendly Investigations**: Expand CACs, Barnahus, and OSCs; ensure access to psychosocial support and legal aid.
- **Protect Privacy and Dignity**: Strengthen safeguards for victim identity, data protection, and trauma-informed care.

9.7 Data, Reporting, and Evidence Management

- **Enhance Reporting Mechanisms**: Ensure anonymous, accessible, and multilingual reporting platforms.
- **Standardize Evidence Handling**: Develop protocols for digital evidence collection, preservation, and sharing.

9.8 Ethical and Human Rights Safeguards

- **Embed Human Rights in Policy**: Ensure all interventions respect privacy, autonomy, and participation rights of children.
- **Oversight and Accountability**: Establish independent oversight bodies for AI, surveillance, and law enforcement actions.

10. Comparative Tables

Table 6: Legal Provisions, Enforcement Models, and International Mechanisms

Country	Key Legislation	Enforcement Mechanism	International Cooperation
India	POCSO Act, IT Act, DPDP Act	Cybercrime Units, I4C, CyTrain, Sahyog	UNCRC, OPSC, MLATs, INTERPOL, INHOPE
USA	PROTECT Act, COPPA, Child Pornography Act	FBI, ICE, NCMEC, ICAC Task Forces	MLATs, INTERPOL, NCMEC, INHOPE
UK	Sexual Offences Act, Online Safety Act	NCA, CEOP, CACs, Barnahus	EUROPOL, INTERPOL, INHOPE, IWF
EU	GDPR, DSA, Sexual Offences Directive	Europol EC3, Barnahus, CACs	Budapest Convention, INHOPE, Europol
Australia	Criminal Code Act, eSafety Act	AFP, eSafety Commissioner, OSCs	Five Eyes, INTERPOL, INHOPE
Brazil	Child and Adolescent Statute	Federal Police, SaferNet	OAS, INTERPOL, INHOPE

11. Case Studies and Lessons Learned

11.1 Supreme Court of India (2024): Just Rights for Children Alliance v. S. Harish

- **Issue**: Whether mere possession or viewing of CSEAM is punishable under POCSO and IT Act.
- **Outcome**: Supreme Court held that accessing, viewing, or possessing CSEAM, even without intent to distribute, constitutes "constructive possession" and is punishable. The judgment clarified the scope of Section 15 of POCSO and Section 67B of the IT Act, strengthening enforcement and closing interpretative gaps.[21]

11.2 Operation Vibora (2024–2025): INTERPOL, Europol, Spanish National Police

- **Action**: Online investigation led to the identification and arrest of 20 suspects across 12 countries, seizure of digital evidence, and identification of 68 additional suspects.

[21] Available at https://research.grhari.com/supreme-court-clarifies-the-scope-of-section-15-of-the-pocso-act-and-section-67b-of-the-it-act-in-child-pornography-cases-just-rights-for-children-alliance-anr-vs-s-harish-ors-2024-insc-716/

The operation demonstrated the effectiveness of international task forces and information sharing.

11.3 Europol VIDTF (2025)

- **Impact**: 51 children identified and safeguarded, 213 leads sent to national authorities, highlighting the value of multinational victim identification and digital forensics.

11.4 Kerala Police (2025): 'Trace an Object' and 'Take it Down' Tools

- **Innovation**: AI-driven tools for victim identification and CSAM takedown, developed through a hackathon, exemplify law enforcement-led technological innovation and public engagement.

11.5 Operation Pacifier (FBI, USA)

- **Method**: Infiltration of a dark web CSAM site using advanced digital forensics and hacking tools, leading to hundreds of prosecutions and global collaboration. The operation raised important legal and ethical questions about privacy and jurisdiction.

12. Conclusion

Law enforcement plays a central, evolving role in preventing online crimes against children. The effectiveness of their efforts depends on robust legal frameworks, specialised training, technological innovation, inter-agency and international cooperation, and a steadfast commitment to child rights and ethical standards. While significant progress has been made—through legislative reforms, multidisciplinary models, AI-driven detection, and global partnerships—persistent challenges remain. These include technical and resource constraints, jurisdictional barriers, privacy concerns, and the rapid evolution of online threats.

A holistic, adaptive, and rights-based approach is essential. This requires continuous investment in capacity building, legislative harmonisation, technology, victim support, and prevention. International cooperation, public-private partnerships, and community engagement are critical to creating a safer digital environment for children. By learning from best practices and model policies across jurisdictions, and by centring the voices and needs of children, law enforcement and policymakers can build resilient systems that protect children from online harm—now and in the future.