IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Role of Law Enforcement in Preventing Online Crimes against Children in India

Chennampalli Nareshbabu
Police constable, Technical Teaching Faculty,
Police Training College, Ananthapuramu,
Andhra Pradesh Police Department, Andhra Pradesh, India.

Abstract: Children's online safety has become a critical national concern as the digital environment exposes them to cyberbullying, online grooming, sexual exploitation, trafficking, financial fraud, and harmful content. This paper examines the pivotal role of police in safeguarding children from online crime at the national level. It analyses the preventive, investigative, and response-oriented functions of law enforcement agencies in addressing cyber offences against children. The study explores the national legal and policy frameworks—such as the Information Technology Act, Bharatiya Nyaya Sanhita, 2023, POCSO Act, and the Cybercrime Prevention against Women and Children (CCPWC) Scheme—that guide police actions in digital child protection.

The abstract further highlights the essential coordination between national police bodies, cyber forensic units, social media platforms, child welfare organizations, and educational institutions in effectively combating online threats. It also discusses the emerging challenges faced by law enforcement, including rapid technological changes, resource limitations, capacity-building needs, encrypted platforms, and darknet-based exploitation. Finally, the paper outlines effective national-level strategies and best practices adopted by the police to strengthen online child safety, enhance digital resilience, and improve protection outcomes across the country.

KEYWORDS

Online cyber Crime, Police, Role of Law Enforcement, Best Strategies Children's online safety, Police role, Child protection, National-level policing, POCSO Act, BNS-2023, IT Act, CCPWC Scheme, Cyber forensic units

INTRODUCTION

Online Crimes against children

Children are among the most vulnerable members of society and face various forms of violence, including sexual abuse, exploitation, trafficking, forced labour, and abduction. Images of child sexual abuse on the internet are not virtual—they represent real crimes against real children. The global reach of the internet has made it easier for offenders to produce, share, and even live stream abuse, while contacting children through social networks, games, or apps. INTERPOL addresses these crimes with an international focus, issuing Yellow Notices to trace missing children and working with member countries to rescue victims of trafficking and forced labour. Its Crimes against Children unit prioritizes identifying and rescuing young victims, blocking access to child sexual abuse material, and preventing sex offenders from traveling abroad to abuse children or evade justice.

Who is Child?

“According to Section 2(1)(d) of the Protection of Children from Sexual Offences (POCSO) Act, 2012, a ‘child’ is defined as any person who is below the age of eighteen years.”

OBJECTIVES OF THE STUDY

- To examine the rapid rise of cyber-crimes against children and their impact.
- To analyze the legal frameworks for child cybercrime protection, including the IT Act, POCSO Act, and Bharatiya Nyaya Sanhita, 2023, and their relevance in addressing different types of offences.
- To explore the role of the government and law enforcement agencies in preventing, detecting, and responding to cybercrimes targeting children.

RESEARCH METHODOLOGY

This study is based on an analytical research approach. The data used for the research were collected from secondary sources, including libraries, newspapers, research papers, LEA’s Portals, journals, and reliable internet sources. All sources consulted are cited in the References section.

What is Cyber Crime?

Cyber crimes are bad things people do using computers, the internet, or other digital devices. They can use the internet as a tool to do wrong, or they might target someone online. Online abuse happens when someone tries to scare, hurt, or make another person feel bad on the internet. This can happen on computers, tablets, or phones. The person doing it could be a stranger, someone they know, an adult, or even another child.

Because the internet is fast, anonymous, and connects people all over the world, it makes it easier for people to do crimes like stealing money, tricking others, bullying, or pretending to be someone else. These crimes can be done by people who know a little about computers or by groups who are very skilled.

What is Cyber/Online Abuse?

Cyber or online abuse is when someone uses the internet, phones, or other digital devices to threaten, hurt, scare, or embarrass another person. If someone feels unsafe or scared online, it counts as cyber abuse. This can happen on computers, tablets, or phones. The person doing it could be a stranger, someone they know, an adult, a child, or even someone hiding their identity.

Why Worry About Cyber/Online Abuse?

Anyone using the internet can face cyber abuse, but children are especially at risk. While kids learn new technologies quickly, they may not always know how to recognize or deal with online dangers.

The first step to staying safe is learning the right words to talk about cyber abuse. Parents, teachers, and caregivers need to understand these risks so they can teach, protect, and help children. Since the internet is a big part of kids’ lives today, it’s always better to be safe than sorry.

Cyber Crimes: An Overview

Children today spend a lot of time online for learning, fun, and connecting with others. While the internet is useful, it also has risks—especially for kids, who can be more vulnerable than adults.

To stay safe, it’s important to know how to spot and report online abuse and follow good digital habits. As we use the internet more, especially since the pandemic, it’s important to be ready to protect ourselves while enjoying online communities and activities.

The following includes the cyber-crimes against children that are being committed in India:-

- **Child Pornography/ Child sexually abusive material (CSAM):** Child sexually abusive material (CSAM) refers to material containing sexual image in any form, of a child who is abused or sexually exploited. Section 67 (B) of IT Act states that "it is punishable for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. https://cybercrime.gov.in/Webform/CrimeCatDes.aspx
- **Cyberstalking and Cyberbullying:** Cyberbullying is when someone sends mean messages, posts hurtful pictures, or spreads false rumors about a person online. Cyberstalking is constantly following or bothering someone online without their permission.
- **Online Grooming:** This happens when an adult or older person tries to befriend a child (and sometimes their family) online to gain trust for the purpose of sexual abuse.
- **Phishing and Online Fraud:** Phishing is when someone sends fake messages to trick a person into giving personal information or accidentally installing harmful software like viruses or ransomware.
- **Exposure to Child Sexual Abuse Material:** This involves sharing, making, or keeping sexually explicit pictures, videos, texts, or emails involving children.
- **Identity Theft and Impersonation:** This is when someone steals personal information and pretends to be another person to do bad things online.
- **Hacking and Malware Attacks:** Hacking is breaking into someone's computer or account without permission. Malware attacks use harmful software to damage computers or steal information.

The latest data released by the National Crime Record Bureau (NCRB) on online Crime against Children

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2022. As per the data published by the NCRB, details of crime head-wise cases registered under cyber crimes against children (below 18 years) during the period from 2018 to 2022 are at Annexure.

Crime Heads-wise Cases Registered under Cyber Crimes against Children (below 18 Yrs.) during 2018-2022.

S.No.	Crime Heads	2018	2019	2020	2021	2022
1	Cyber Blackmailing/Threatening/Harassment	4	3	3	23	74
2	Fake Profile	3	2	1	9	2
3	Cyber Pornography/ Hosting or Publishing Obscene Sexual Materials depicting children	44	103	738	969	1171
4	Cyber Stalking/Bullying	40	44	140	123	158
5	Internet Crimes through Online Games etc	0	1	0	0	2
6	Other Crimes against Children	141	153	220	252	416
7	Total Cyber crimes against Children	232	306	1102	1376	1823

Source: 29 JUL 2025 5:11PM by PIB Delhi

Rising Crimes Against Children in India: NCRB 2023 Report

1. Overall Crime Against Children

In 2023, 1,77,335 cases of crimes against children were registered, a 9.2% increase over 2022 (1,62,449) and 2021 (1,49,404). The crime rate rose to 39.9 per one-lakh child population. Major crimes included Kidnapping and Abduction (79,884 cases, 45%) and POCSO Act violations (67,694 cases, 38.2%). Victims included 762 below 6 years, 3,229 aged 6–12, 15,444 aged 12–16, and 21,411 aged 16–18, totaling 40,846, mostly girls.

2. Offenders, Other Crimes, and Regional Distribution

Most offenders were known to the victims (39,076 cases), including family members (3,224), acquaintances/employers (15,146), and friends/online contacts (20,706). Kidnapping for forced marriage involved 14,637 girls. Other crimes included 1,219 murders, 3,050 simple hurt cases, and 373 abetments to suicide. Special laws contributed 6,038 cases under the Child Marriage Act and 1,390 under the Child Labour Act. Highest cases by state: Madhya Pradesh (22,393), Maharashtra (22,390), Uttar Pradesh (18,852), Assam (10,174), with Delhi (7,769) and Andaman & Nicobar Islands having high rates.

3. Police Action and Online/Cyber Crimes

Out of 2,57,756 cases investigated, 1,12,290 were charge-sheeted, with 80,198 pending (32.2% pendency). Charge-sheet rates varied, high in Tamil Nadu (93.7%) and Andhra Pradesh (91.3%), low in Delhi (31.7%) and Haryana (39.6%). Cyber crimes targeting children—including online sexual exploitation, grooming, and abuse—are rising, with offenders using social media, chat apps, and online games. National initiatives like the Indian Cyber Crime Coordination Centre (I4C), Cyber Crime Reporting Portal (www.cybercrime.gov.in), and helpline 1930 help report, investigate, and prevent online crimes against children.

LEGAL PROVISIONS AND REDRESSAL

In India, there are laws to protect children from cybercrimes and online abuse. The IT Act, 2000 deals with crimes committed using computers and the internet. The POCSO Act, 2012 protects children from sexual offences, including online sexual abuse. Some sections of the BNS also cover cybercrimes. These laws help children stay safe online and provide ways to report and take action against offenders.

A. Legal Provisions Pertaining to Cybercrimes

Cybercrime	Relevant Law/Sections
Cyberstalking	Sec 11(iv) POCSO Act, Sec 78, 79 BNS, Sec 66, 66A/C/D IT Act, 2000
Phishing	Sec 66, 66A/C/D IT Act, 2000
Cyberbullying	Sec 351(1), 351(2)/(3),351(4) BNS
Identity Theft	Sec 66C IT Act
Violation of Privacy	Sec 66E, 72 IT Act, Sec 23 POCSO Act
Hacking	Sec 43, 66 IT Act
Child Pornography	Sec 11(v)&(vi), 13/14/15 POCSO Act, Sec 66E, 67 IT Act, Sec 294 BNS
Online Grooming	Sec 11(vi) POCSO Act, Sec 67B(c) IT Act
Online Child Trafficking	Sec 5 ITPA, Sec 96 BNS
Online Extortion	Sec 308(1), 308(2), 308(3), 308(4), 308(5), 308(6), 308(7) BNS
Defamation	Sec 356(1)/351(2)/336(4) BNS
Online Sexual Harassment	Sec 11 POCSO Act, Sec 75, 79 BNS
Sexting	Sec 67, 67A IT Act, Sec 11,12 POCSO Act

HOW TO FILE A COMPLAINT?

As a child, if you experience or come across online abuse, talk to your parents, guardians, or a teacher, who can guide and support you through the reporting process. While you can approach authorities yourself, it is recommended to seek help from trusted adults. Cybercrimes can be reported through online portals like the National Cyber Crime Reporting Portal or NCPCR's 'POCSO E-box', or by directly approaching a local police station or cybercrime cell. Under Section 173 of Bharatiya Nagarik Suraksha Sanhita, 2023, police must record your complaint regardless of where the crime occurred. For online sexual offences, caregivers are required to report under the POCSO Act, and free legal aid is available to victims and their guardians.

There are several mechanisms to report cybercrimes. Some of the options available to you are depicted below:

Children who experience or witness online abuse can report it through multiple channels. The POCSO e-box (by NCPCR) allows registration of sexual harassment cases online (link), while the Child line 1098 helpline provides toll-free support for abuse, neglect, or cyber offences. Complaints can also be made at any local police station, cyber police station, or to state-appointed cyber cell officers. Schools are required to have a Child Abuse Monitoring Committee (CAMC), where any known offence, including online abuse, must be reported; the committee will forward it to authorities after enquiry.

Children and guardians can also access legal counseling and support through centers like Ask Crisis Line (8793088814), She Will Survive, Orinam, Centre for Cyber Victim Counseling, and Cyberjure Legal Consulting. For broader child protection, Child Welfare Committees (CWCs) and statutory bodies like NCPCR and SCPCRs can be approached. Additional help is available via NGO helplines, including the CyberPeace Foundation (helpline@cyberpeace.net, +91 95700 00066) and the National Cyber Crime Reporting Helpline (1930).

UN CONVENTION ON THE RIGHTS OF THE CHILD (UNCRC)

The UNCRC, adopted in 1989, is a legally binding international treaty protecting the rights of all children, regardless of race, religion, or abilities. Ratified by 196 countries, it obliges governments to ensure children’s survival, development, education, protection from harm, and participation in decisions affecting them.
It is guided by four principles:

- Non-discrimination – All children have equal rights.
- Best interests of the child – Decisions must prioritize children’s welfare.
- Right to life, survival, and development – Access to healthcare, education, and safe environments.
- Respect for the views of the child – Children’s opinions must be considered.

The Convention also covers protection from abuse and exploitation, family life, identity and participation, and special protection for vulnerable children. Optional protocols address child recruitment in armed forces, child prostitution and pornography, and direct reporting of rights violations to the UN Committee.

KEEPING CHILDREN SAFE ONLINE

UNICEF India and NASSCOM Foundation partner online safety of children Tech-based innovations for child rights in India

UNICEF India and NASSCOM Foundation signed an MoU to engage the IT-BPM sector in promoting child rights, focusing on child online protection and encouraging innovations for child welfare. Digital technologies offer children opportunities for learning, play, and socialization, but lack of digital literacy exposes them to cybercrime, abuse, and exploitation. Through this partnership, both organizations aim to raise awareness among parents, teachers, and children, helping them navigate the digital space safely via workshops, webinars, Tweet chats, and roadshows.

The collaboration also emphasizes technology for social good, aligning with the UN Agenda 2030 and Sustainable Development Goals. NASSCOM Foundation will include a new category on tech-based innovations for child rights, addressing issues like malnutrition, education, and adolescent empowerment. The partnership encourages stakeholders, including schools, IT-BPM companies, and governments, to use technology responsibly as a learning tool while safeguarding children from online risks.

Advice for Parents and Children on Staying Safe Online

For Parents:

Develop an open and honest dialogue with your children about social media, apps, games, and the Internet. Encourage safe habits and discuss the difference between “good” and “bad” content. Show interest in their online activities, set rules, and lead by example. While filtering and reporting tools help, they do not solve all problems—children should feel comfortable approaching you if they feel threatened or uncomfortable. Reduce overexposure to online content, as even everyday photos can be misused. Seek support from authorities, educators, or specialist groups when needed.

For Children and Teenagers:

Privacy: Control your devices, information, and passwords; review privacy settings regularly; don’t share personal details like full name, address, or school.
Online Friends: Be cautious with online friends; never meet them offline without informing an adult and taking safety precautions.
Think Before You Share: Consider the messages or images you post; once online, you lose control over them. Trust your instincts and avoid uncomfortable interactions.
Report: Record and report any threatening or inappropriate content to someone you trust or to authorities. If targeted by blackmail or threats, stop all contact and seek help. Useful reporting platforms include national police authorities and sites like www.inhope.org

THE POLICE'S ROLE IN COMBATING AND PREVENTING CYBER CRIME AGAINST CHILDREN

‘Police’ and ‘Public Order’ are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cybercrime through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

To strengthen the mechanism to deal with cyber crimes, including cyber crimes against women and children in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

i. The Ministry of Home Affairs has provided financial assistance under the ‘Cyber Crime Prevention against Women and Children (CCPWC)’ Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs’ personnel, public prosecutors and judicial officers.

ii. Cyber Forensic-cum-Training Laboratories have been commissioned in 33 States/UTs. As per available information, Cyber Forensic-cum-Training Laboratory has not been established in Tamil Nadu under CCPWC scheme.

iii. Training curriculum has been prepared for LEA personnel, Public Prosecutors and Judicial officers for better handling of investigation and prosecution. States/UTs have been requested to organize training programmes. More than 24,600 LEA personnel, Public Prosecutors and Judicial officers have been provided training on cyber crime awareness, investigation, forensics etc. under CCPWC Scheme.

iv. The Ministry of Home Affairs has set up the ‘Indian Cyber Crime Coordination Centre’ (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.

v. The ‘National Cyber Crime Reporting Portal’ (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.

vi. Memorandum of Understanding (MoU) has been signed on 26.04.2019 between the National Crime Records Bureau (NCRB), India and the National Center for Missing and Exploited Children

(NCMEC), USA regarding receiving of Tipline report on online child pornography and child sexual exploitation contents from NCMEC. So far, more than 69 lakhs Cyber Tipline reports have been shared with concerned States/UTs.

vii. In exercise of the powers conferred by clause (b) of sub-section (3) of section 79 of the Information Technology Act 2000, Central Government being the appropriate government designated the Indian Cyber Crime Coordination Centre (I4C), to be the agency of the Ministry of Home Affairs to perform the functions under clause (b) of sub-section (3) of section 79 of Information Technology Act, 2000 and to notify the instances of information, data or communication link residing in or connected to a computer resource controlled by the intermediary being used to commit the unlawful act on 13.03.2024.

viii. National Cyber Forensic Laboratory (Evidence) was inaugurated on 14.05.2022 at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and reduced turnaround time by 50%.

ix. The state of the art ‘National Cyber Forensic Laboratory (Investigation)’ has been established, as a part of the I4C, at New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) has provided its services to State/UT LEAs in around 11,835 cases pertaining to cyber crimes.

x. A State of the Art Centre, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.

xi. Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi-jurisdictional issues by on boarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh.

xii. Samanvaya Platform has been made operational to serve as an Management Information System(MIS) platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics based interstate linkages of crimes and criminals, involved in cybercrime complaints in various States/UTs. The module ‘Pratibimb’ maps locations of criminals and crime infrastructure on a map to give visibility to jurisdictional officers. The module also facilitates seeking and receiving of techno-legal assistance by Law Enforcement Agencies from I4C and other SMEs. It

has lead to arrest of 6,046 accused, 17,185 linkages and 36,296 Cyber Investigation assistance request.

xiii. ‘Sahyog’ Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act.

xiv. To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c), Radio campaign, caller tune, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, newspaper advertisement on digital arrest scam, announcement in Delhi metros on digital arrest and other modus operandi of cyber criminals, use of social media influencers to create special posts on digital arrest, digital displays on railway stations and airports across, etc.

CONCLUSION

With the rapid growth of digital technology, children are increasingly exposed to online risks such as cyberbullying, sexual abuse, and harassment. It is essential for children to be aware of these dangers and for adults to provide guidance and support. Various legal frameworks, including the POCSO Act, BNS provisions and the IT Act, along with reporting mechanisms like the POCSO e-box, Child line 1098, police/cyber cells, school committees (CAMC), CWCs, and statutory commissions (NCPCR/SCPCRs), provide comprehensive avenues for redressal and protection.

The combination of awareness, legal provisions, reporting channels, and counseling services ensures that children can safely report abuse and receive timely intervention. Empowering children to speak up, involving trusted adults, and strengthening institutional and legal support are key to creating a safe digital environment where children's rights, well-being, and dignity are protected.

REFERENCES

- https://www.unicef.org/india/press-releases/unicef-india-and-nasscom-foundation-partner-online-safety-children-tech-based, Last accessed: 12.12.2025
- https://www.interpol.int/en/Crimes/Crimes-against-children, Last accessed: 12.12.2025
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2149788&reg=3&lang=2, Last accessed: 12.12.2025
- https://www.thehindu.com/news/national/ncrb-report-crime-against-children-rise-in-2023/article70112771.ece, Last accessed: 12.12.2025
- https://ciet.ncert.gov.in/storage/app/public/files/14/cyber-safety/HandbookDigitalSafetyForChildren_English.pdf, Last accessed: 12.12.2025
- https://www.savethechildren.org.uk/what-we-do/childrens-rights/united-nations-convention-of-the-rights-of-the-child, Last accessed: 12.12.2025
- https://www.interpol.int/en/Crimes/Crimes-against-children/Keeping-children-safe-online, Last accessed: 12.12.2025
- https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2110359&reg=3&lang=2, Last Accessed on 20, December 2025