गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Indian Cyber Crime Coordination Centre
सहवीर्यं करवावहै • Working Together With Vigour

# Contextualising Online Crimes Against Women and Children


**Presented By:**

**Aishwarya Dongre IPS**
**Online Crime Against Women and Children (OCWC) Wing**
**Indian Cyber Crime Coordination Centre (I4C)**
**Ministry of Home Affairs**

# I4C Key Focus Areas

Indian Cyber Crime Coordination Centre
सहवीर्य करवावहै • Working Together With Vigour

## Cybercrime Reporting

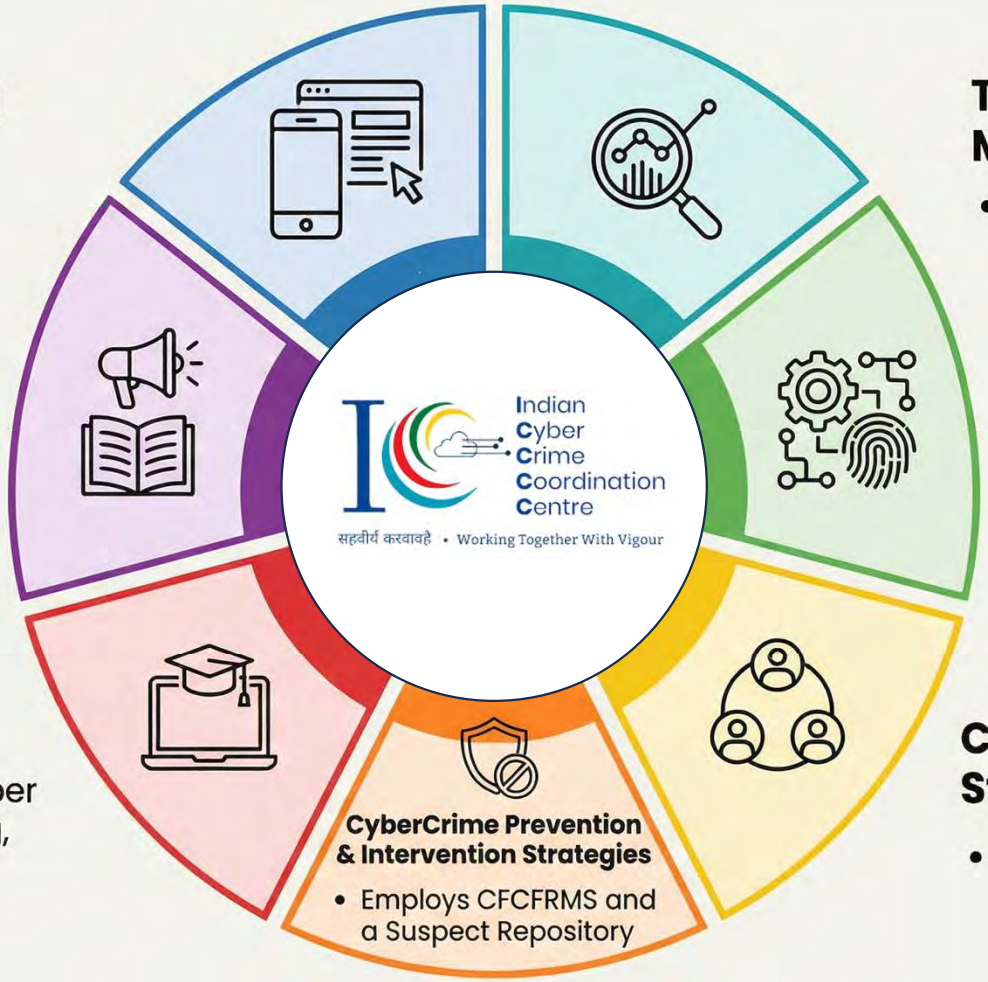
- Utilizes NCRP (cybercrime.gov.in)
- Helpline 1930
- OCWC reporting

## Public Awareness – Cyber Literacy

- Promoted through the CyberDost initiative

## Capacity Building

- Conducted via CyTrain, Cyber Commandos, Peer Learning, State Connect, and Thana Connect




## Threat Analytics And Monitoring

- Identifies Crime Linkages and Hotspots through Sahyog Portal and Pratibimb

## Cyber Investigation Coordination & Support

- Facilitated by Samanvay, NCFL, and Telecom Blocking

## Coordination Among Stakeholders

- Managed through CFMC, Samanvay, and OCWC

# Current Reporting mechanisms

**VICTIMS**

To LEA's and on *National Cyber Crime Reporting Portal*

(Can report anonymously)

- Content so reported can also be taken down/blocked through Sahyog Portal

**3RD Party organizations**

To LEA's and on National Cyber Crime Reporting Portal

(Can report anonymously)

**IT intermediaries**

only to **NCMEC** (private U.S based NGO), no reporting to Indian LEA's or frameworks

(*Just right for children alliance and anr Vs S.. Harish and ors judgement has mandated reporting to Indian SPJU's as well)*

# Indian statutory frameworks

**a) Bhartiya Nyaya Sanhita (BNS)**

- **Section 65**: Abuse of a woman below 16 / girl victim below 12
- **Section 70** – Gang rape of a girl below 18 years of age
- **Secs 75,77,78,79**: Sexual harassment, voyeurism, stalking (graded punishments).
- **Section 356:** Deals with defamation, including online defamation.
- **Section 351:** Addresses criminal intimidation through anonymous communication.

**b) The Information Technology Act, 2000 includes provisions to address cybercrimes against women and children:**

- **Section 66C:** Addresses identity theft, with penalties of up to three years in prison and fines.
- **Section 66E:** Covers privacy violations through unauthorized capturing or transmitting images, punishable by up to three years in prison or fines.
- **Section 67 and 67A:** Deal with the transmission of obscene and sexually explicit content, imposing imprisonment and fines for offenders
- **Sec 67B** - Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

**c) Section Sec 11–16, 19–20 of the Protection of Children from Sexual Offences Act, 2012 (POCSO) -** Address online child sexual abuse, grooming, and reporting obligations

**d) Indecent Representation of Women (Prohibition) Act, 1986**- Prohibits depiction of women in an indecent manner across electronic and digital platforms

# International Framework

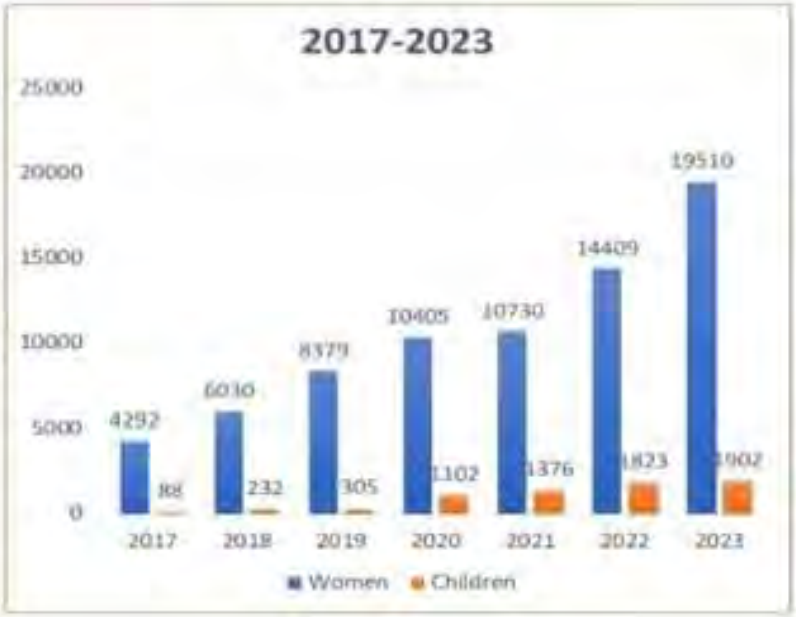
## Un Convention on Cybercrime

- **Article 14.** Offences related to online child sexual abuse or child sexual exploitation material.
- **Article 15.** Solicitation or grooming for the purpose of committing a sexual offence against a child [agreed ad referendum] .
- **Article 16**. Non-consensual dissemination of intimate images of children below the age of 18 years.
- **Article 53. Preventive Measures - -** Each State Party shall take appropriate measures, within its means and in accordance with fundamental principles of its domestic law, to promote the active participation of relevant individuals and entities outside the public sector….. as well as making efforts to ensure the swift removal of child sexual abuse and child sexual exploitation material;

# Cyber Crime against Women & Children

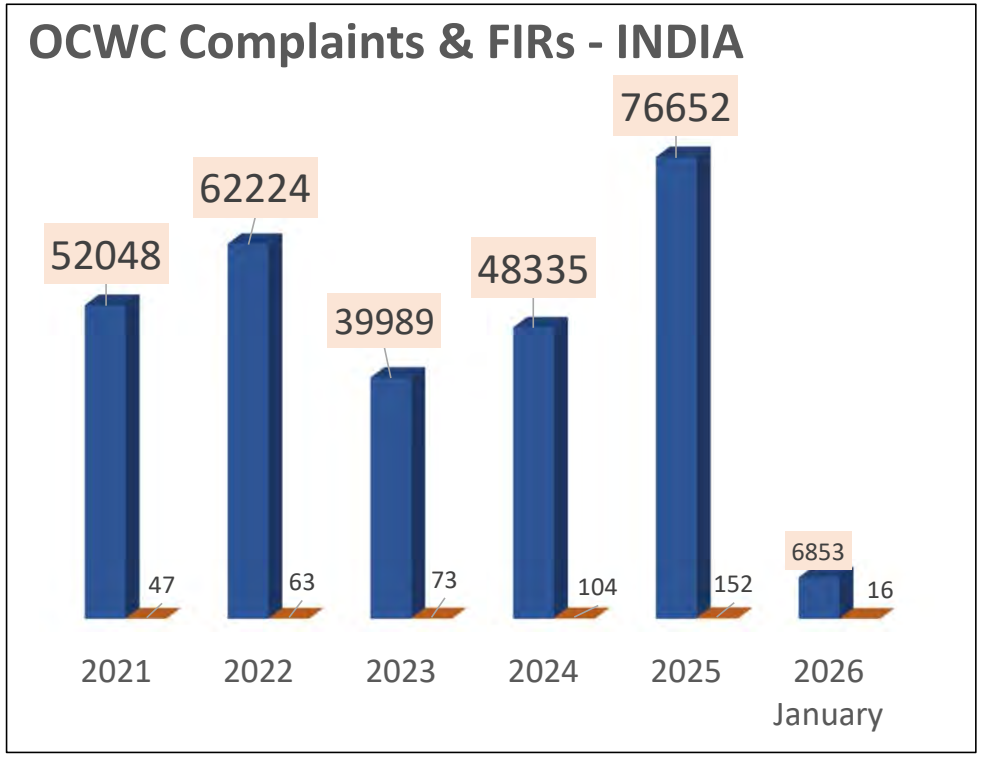
## All India States UTs (2017-2023)

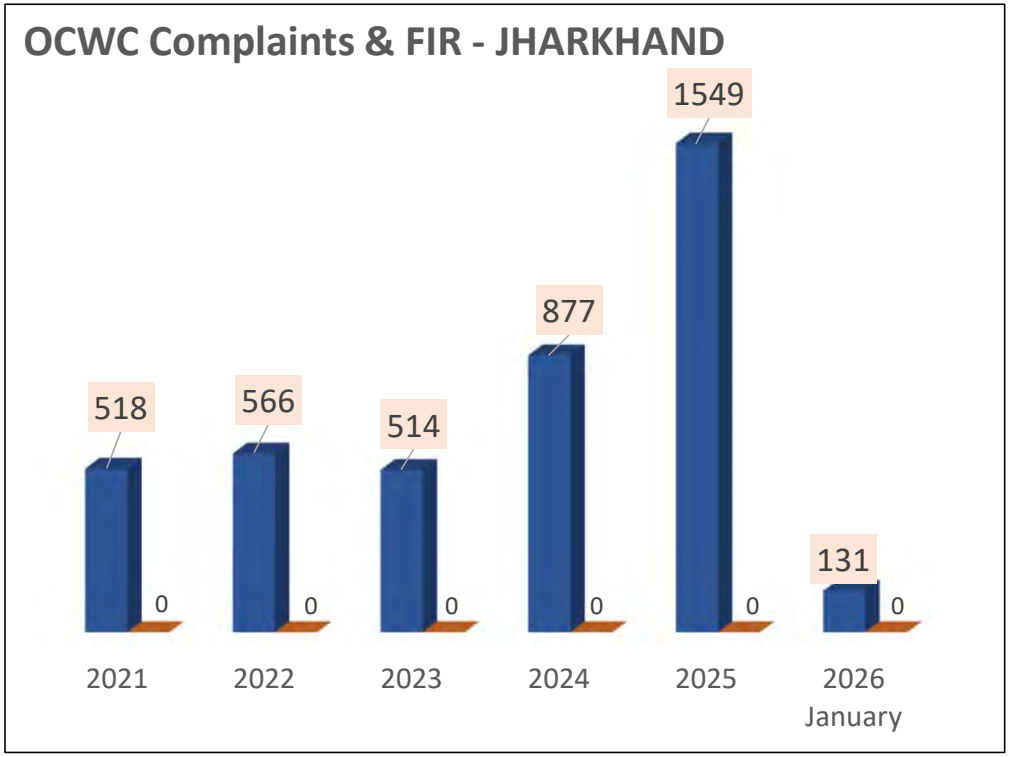
| Year | Total Cyber Crimes registered | Total Cyber Crimes against Women Registered | Total Cyber Crimes against Children Registered | Percentage of total nos of Cybercrimes against Women and Children with the total nos of Cybercrimes reported |
|---|---|---|---|---|
| | A | B | C | D (B+C/A) |
| **2017** | 21,796 | 4242 | 88 | 19.87% |
| **2018** | 27,248 | 6030 | 232 | 22.98% |
| **2019** | 44,546 | 8379 | 305 | 19.49% |
| **2020** | 50,035 | 10405 | 1102 | 22.99% |
| **2021** | 52,974 | 10730 | 1376 | 22.85% |
| **2022** | 65,893 | 14409 | 1823 | 24.63% |
| **2023** | 86,420 | 19510 | 1902 | 24.77% |




Source: Crime in India, 2023

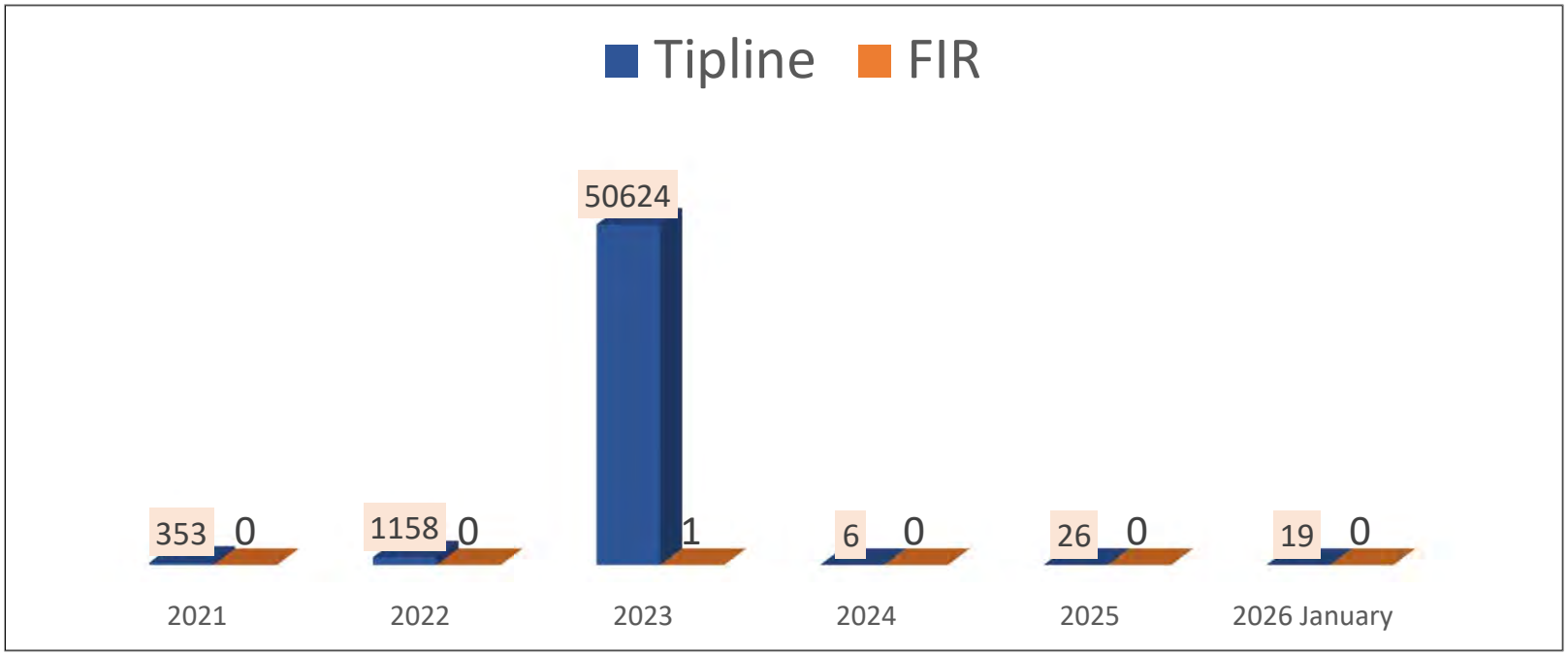
# Online Crime Against Women and Children Centre



# Online Crime Against Children (Tipline) Centre

## NCEMC Tipline with FIR statistics - Jharkhand



# OCWC NCRP Complaint Statistics – Jharkhand

1st January to 31st December 2025

## 1. TOTAL COMPLAINTS

| S. No. | Category | Anonymous | Report & Track |
|---|---|---|---|
| 1 | CSEAM - | 213 | 38 |
| 2 | Rape/Gang Rape (RGR)- | 141 | 44 |
| 3 | Sexually Explicit Act | 245 | 93 |
| 4 | Sexually Obscene material | 562 | 202 |
| | **Total** | **1161** | **377** |
| | **Grand Total** | **1538** | |

## 2. STATUS OF COMPLAINTS

| Status | Anonymous | Report & Track |
|---|---|---|
| **Under Process** | 18 | 07 |
| **Closed** | 0 | 0 |
| **Registered** | 1143 | 370 |
| **Rejected** | 0 | 0 |
| **FIR Registered** | 0 | 0 |
| **Total** | **1161** | **377** |
| **Grand Total** | **1538** | |

## 3. TOP HOTSPOT DISTRICT

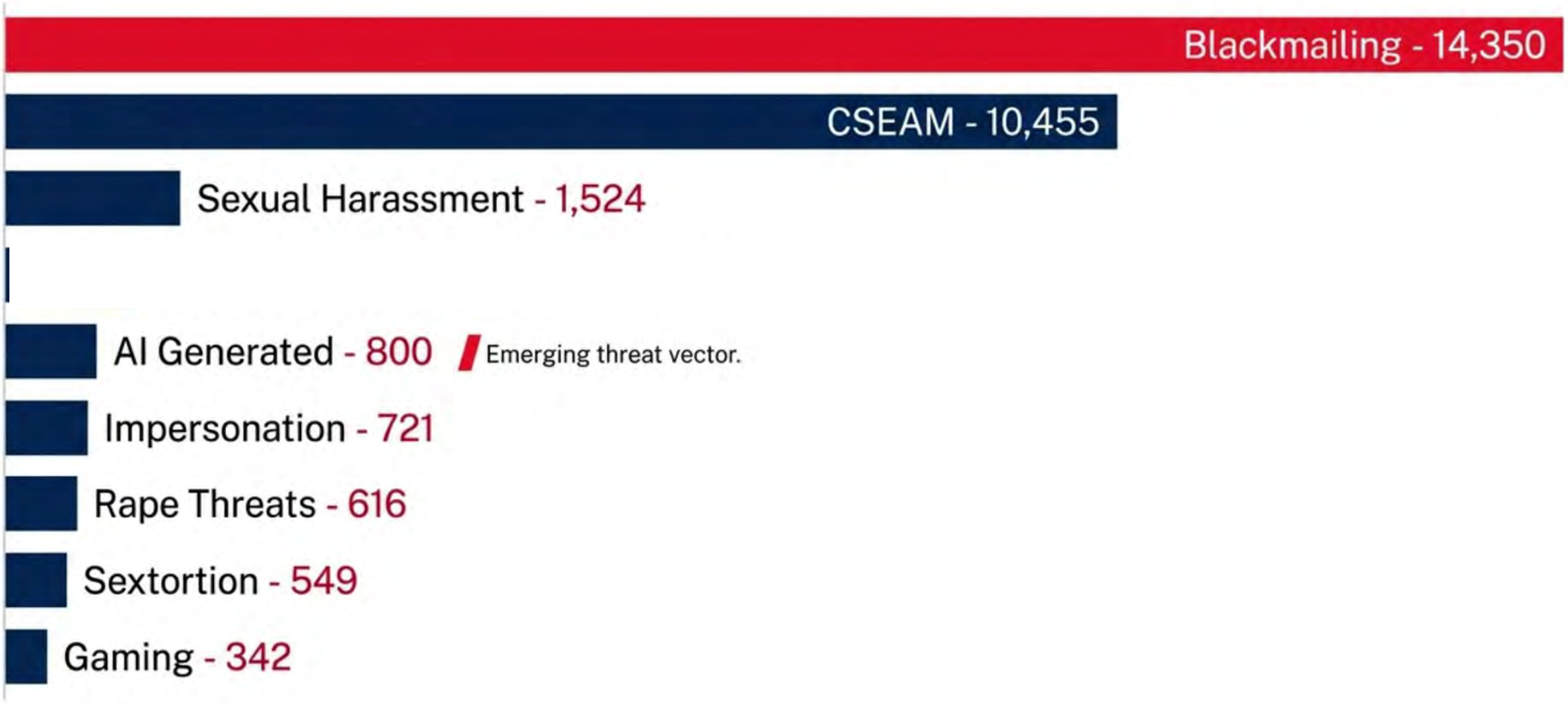
| | Anonymous | |
|---|---|---|
| S No. | District | Complaints |
| 1 | RANCHI | 274 |
| 2 | JAMSHEDPUR | 205 |
| 3 | DHANBAD | 137 |
| 4 | BOKARO | 109 |
| 5 | HAZARIBAGH | 59 |
| 6 | DEOGHAR | 53 |
| 7 | PALAMAU | 46 |
| 8 | GIRIDIH | 41 |
| 9 | SAHEBGANJ | 25 |
| 10 | RAMGARH | 24 |

| | Report & Track | |
|---|---|---|
| S No. | District | Complaints |
| 1 | RANCHI | 101 |
| 2 | JAMSHEDPUR | 56 |
| 3 | DHANBAD | 50 |
| 4 | BOKARO | 28 |
| 5 | RAMGARH | 19 |
| 6 | HAZARIBAGH | 19 |
| 7 | GIRIDIH | 13 |
| 8 | DEOGHAR | 12 |
| 9 | CHAIBASA | 10 |
| 10 | SARAIKELA | 9 |

## 5. TYPE OF COMPLAINTS

| S.N. | Type of Complaint | Complaint |
|---|---|---|
| 1 | Blackmailing | 329 |
| 2 | CSEAM | 251 |
| 3 | Loan Harassment | 82 |
| 4 | Sexual Harassment | 29 |
| 5 | AI Generated | 24 |
| 6 | Rape Threats | 17 |
| 7 | Impersonation | 12 |
| 8 | Sextortion | 08 |
| 9 | Gaming | 03 |

# Top Complaint Categories: The Methods of Victimization



# Seven Emerging Trends in Online Crimes Against Women and Children

**CSEAM: Commercial Exploitation Material**

**Gaming: Grooming & Cyber Harassment**

**NCII: Non-Consensual Intimate Imagery**

**Catfishing: Online Deception**

**Doxxing: Public PII Exposure**

**LSAC: Live-streaming Abuse**

**FSEC: Financial Sextortion**

# The Modern Offender's Tech Stack

# NHRC Advisory (2023) on CSEAM: Key Highlights

1

**Legal Reform**:

Replace term "Child Pornography" with "CSEAM", broaden intermediary definitions, adopt UN Convention against cybercrime.

2

**Platform Regulation**:

Mandate tech-based CSEAM detection, 6-hour takedown rule, enforce KYC & data sharing.

3

**Investigation Support**:

Form specialized police units, create national CSEAM database, enhance forensic capacity.

4

**Awareness & Victim Aid**:

Train LEAs, run public awareness drives, integrate cyber safety in schools, offer victim support.

# **SC POCSO Judgement POCSO and CSEAM :** Just Rights For Children Alliance & Anr Versus S. Harish & ORS dtd 23.09.24

The intermediaries should be made more accountable of CSEAM content on their platforms.

They should mandatorily flag such content and take efforts on pulling down such content – proactively as well as on the information given by LEAs.

They should report this content to local LEAs, Special Police Juvenile Units, cybercrime portal for taking necessary enforcement action.

The report to local LEAs, SPJUs, cybercrime portal by Intermediaries shall include the details of the device in which such pornographic content was noticed and the suspected device from which such content was received.

# KEY TECHNICAL INITIATIVES & TOOLSETS

## SAHYOG PORTAL

**Function:**
Intermediary Integration

**Goal:**
Improve takedown/blocking and facilitate direct reporting by platforms to Indian agencies.

## CDAC MONITORING TOOL


**Function:**
AI-Based Detection

**Goal:**
Automatically identify and segregate confirmed CSEAM content for focused operations.

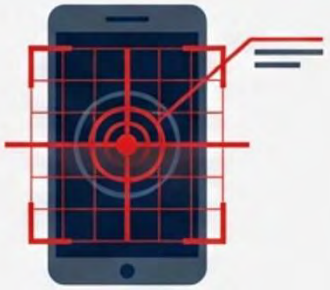
## NATIONAL HASH DATABASE


**Function:**
Digital Fingerprinting

**Goal:**
A permanent repository to prevent the resurfacing of illegal content across different platforms.

# INTELLIGENCE & VULNERABILITY ASSESSMENT

## THREAT ANALYTICS: APP VULNERABILITY



SCANNING

Identified High-Risk Platforms:

**ROBLOX**

**TANGO APP**

Providing vulnerability assessment reports to seal loopholes.

## DATA-DRIVEN INTEL: TARGET IDENTIFICATION


DATASET ANALYSIS

Assisting States in identifying:

1. Online Child Abuse Content Creators
2. Repeat Offenders

## CURRENT MOMENTUM: JANUARY 2026 SNAPSHOT

Data indicates no slowdown in volume for the new year.

| TIPLINES RECEIVED | RUN ON PMT |
|---|---|
| 232,582 | 83,285 |
| January 2026 Only. | |

| UPLOADED ON NCRP | FIRS REGISTERED |
|---|---|
| 1,160 | 234 |

## TARGETING THE OFFENDERS

Results of Focussed Data-driven Intelligence

**167**

ONLINE CHILD ABUSE CONTENT CREATORS IDENTIFIED

**172**

REPEAT OFFENDERS IDENTIFIED

## 2025 SNAPSHOT

**Tiplines on NCRP – 5442**

**FIRs - 594**

# Cross-Border Takedown: A Cybercrime Case Study

An international tip-off from US Homeland Security about illegal content triggered a successful domestic investigation in India.

## STEP 1: THE TIP-OFF


### US Agency Flags Suspect

A case initiated by US Homeland Security Investigations (HSI) at Los Angeles Airport found CSEAM content linked to an Indian national.

## STEP 2: THE INVESTIGATION

### India's Digital Manhunt

I4C and Rajasthan Police identified of suspects:

- **40** email IDs
- **47** social media accounts
- **30** mobile numbers

## STEP 3: THE OUTCOME

### Actionable Intelligence Uncovered

- Confirmed **12** NCMEC tiplines
- Identified **186** related financial transactions in India.

Criminal case registered in **Rajasthan** and **2 suspects arrested**.

# OPERATIONAL OVERVIEW AND KEY OUTCOMES

## TRIGGER EVENT

Interception at Los Angeles Int'l Airport (Jan 24, 2024)

## TOTAL SEIZURE

**697.24 GB**

of CSAM content across 11,883 files

## FINANCIAL SCOPE


15+ Lakhs INR estimated involvement. Confirmed global payments from 5+ countries.

## NETWORK IDENTIFIED

08 Sellers, 29 Receivers

## ENFORCEMENT ACTION

3 FIRs Registered. 4 Adults Arrested. 2 Juveniles Detained.

# GEOGRAPHIC DISTRIBUTION OF THE DOMESTIC NETWORK


**LEGEND:**
Red = Primary Source/Seller Hub.
Blue = Recipient/Buyer Locations.

# JUDICIAL OUTCOME AND SEVERITY OF OFFENSE

## “Owing to the gravity of the offense, they were denied bail by the concerned courts for 6 months.”

- Accused were forced to approach the High Court for relief.
- The judicial system recognized the operation as an organized network of commercial CSAM spanning across states, rather than isolated incidents.

# Sample Complaint - 01

**Nature of Complaint: Blackmailing / Sextortion**

| | |
|---|---|
| **Acknowledgement No.** | 13401250000055 |
| **Category of Complaint** | Sexually Obscene material |
| **Sub Category of Complaint** | |
| **Additional Information Presently Content** | Yes |
| **Incident Date/Time** | 19/01/2025 0 : 0 : AM |
| **IP Address** | 106.78.0.138 |

## Suspect Details

| Suspect Photo |
|---|
| suspectid_202501201059406644628.png |

| | |
|---|---|
| **State** | JHARKHAND |
| **District** | [redacted] |
| **Pincode** | |
| **Complaint Additional Info** | Mai 17 saal ki hu yeh mera boyfriend hai jo meri private photo rakhke usse mujhe blackmail kar rha hai mai yeh apne ghr walo ko nahi bata skti isisliye mai yeh complaint file kr rhi hu voh mujhe dhamki deta hai ki voh mere private photos viral kar dega or uske badle Mai usko paise chaiye voh paiso ki demand karta hai or paisa nahi Dene pe photo viral karne ki dhamki deta hai bohot time se or mai nahi chhati ki yeh baat mere ghr pe pata chale isisliye mai yaha complaint file kar rhi hu mai abtk usko 1000 de chuki hu pr bhi voh mujhse or paiso ki demand kar rha hai or viral karne ki dhamki de rha mai chhati hu yeh chij mere ghr pe pata naa chale please |

### Supporting Evidence :

| S.No. | Description | Text Information | Supporting Evidence |
|---|---|---|---|
| 1 | WhatsApp | [redacted] | Evidence20250120104215372630 5.png |

# Sample Complaint - 02

**Nature of Complaint: CSEAM Information**

**Complaint Type :** Anonymous (Complaint Registered By Citizen)

| | |
|---|---|
| **Acknowledgement No.** | 13406250000418 |
| **Category of Complaint** | CSEAM - Child Sexual Exploitative and Abuse Material |
| **Sub Category of Complaint** | |
| **Additional Information Presently Content** | Yes |
| **Incident Date/Time** | 17/06/2025 1 : 12 : PM |
| **IP Address** | 49.37.25.211 |

## Suspect Details

| Suspect Photo |
|---|
| suspectid_202506171320416561900.png |

| | |
|---|---|
| **State** | JHARKHAND |
| **District** | [redacted] |
| **Pincode** | |
| **Complaint Additional Info** | there is someone selling cp (child- por-) on telegram i order to investigate bout it i gave him a bait here is the bank account details check this number and his phone its filled with thousands of c- p- videos he was trying to sell me forcefully and share his qr code his named is Akhlesh Meena as shown in bank id |

## Supporting Evidence :

| S.No. | Description | Text Information | Supporting Evidence |
|---|---|---|---|
| 1 | Telegram | 7690920976@ptsbi | Evidence20250617131731361785 5.png |

## Case Study: 01

**Report Name: Intelligence Report on hotpic.one website Hosting Child Sexual Exploitative and Abuse Material (CSEAM)**

- **Ack. No.** 13405250000369
- **Category:** Sexually Obscene material
- **Date of Complaint:** 23/05/2025
- **Status:** Under Process
- **Shared With:** Jharkhand Police
- **Findings:** 02 telegram sellers of CSEAM and 02 UPI IDs
- **Action by State:** 02 accused arrested by Jharkhand Police

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Centre

*Confidential*

File No. 22003/236/2025-OCWC-I4C

(Threat Analysis Report)

HOTPIC ALERT

**Intelligence Report on hotpic.one website Hosting Child Sexual Exploitative and Abuse Material (CSEAM)**

**Prepared By**

Indian Cyber Crime Coordination Centre (I4C)
Ministry of Home Affairs (MHA)
Government of India
Published On: 2nd September 2025

Helpline No. 1930 www.cybercrime.gov.in

**Criminal Investigation Department, Jharkhand, Ranchi**

**Press Release**

**Date: 19.09.2025**

**Criminal Investigation Department, Jharkhand Police cracks Down on Child Sexual Exploitation Network; Two Arrested for Circulating CSEAM through Website & Telegram**

**CID , Jharkhand Police in coordination with Indian Cyber Crime Coordination Centre (I4C),Ministry of Home Affairs, Government of India** has uncovered a major case of Child Sexual Exploitative and Abuse Material (CSEAM) being circulated online through the website *https://hotpic.one/* and allied platforms.

The investigation revealed that the website was being misused as a digital marketplace where child sexual exploitation material was uploaded, distributed, and monetized. Further analysis indicated that offenders were leveraging **Telegram channels** and cloud storage platforms (including MEGA) to sell and disseminate such exploitative content in an organized manner, posing a grave threat to child safety.

Acting swiftly on inputs received through complaints on the National Cybercrime Reporting Portal (NCRP), the Cyber Police registered a case. One of the complaints, from Jharkhand, highlighted a distressing incident where a victim's explicit photos and videos were uploaded on the site without consent, leading to severe psychological trauma and suicidal thoughts.

During the course of investigation, the police successfully identified and apprehended two accused persons –

**1)Ankit Kumar JD and**

**2) Vivek Kumar both from Gandhinagar, Bokaro, Jharkhand.**

On search of their digital devices, a large volume of child sexual abuse material was recovered from their photo gallery. It was further established that they were actively selling these obscene materials through **Telegram groups and sharing MEGA cloud links to buyers**. Shockingly, the network extended internationally, with content being supplied **to foreign citizens in Oman, Bangladesh, and UAE.**

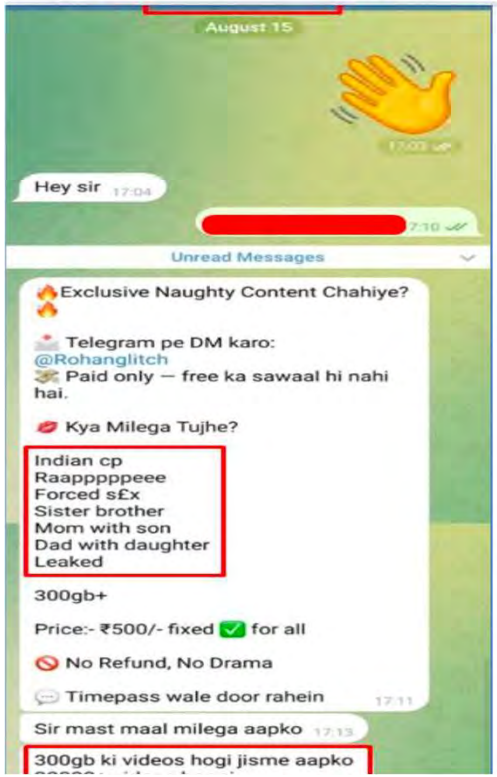
The arrests mark a significant breakthrough in the fight against online child exploitation. Efforts are ongoing to identify and dismantle the wider network of offenders, both within India and abroad. Jharkhand Police is working in close coordination with I4C and relevant international agencies to ensure that such heinous crimes are curbed and offenders are brought to justice.

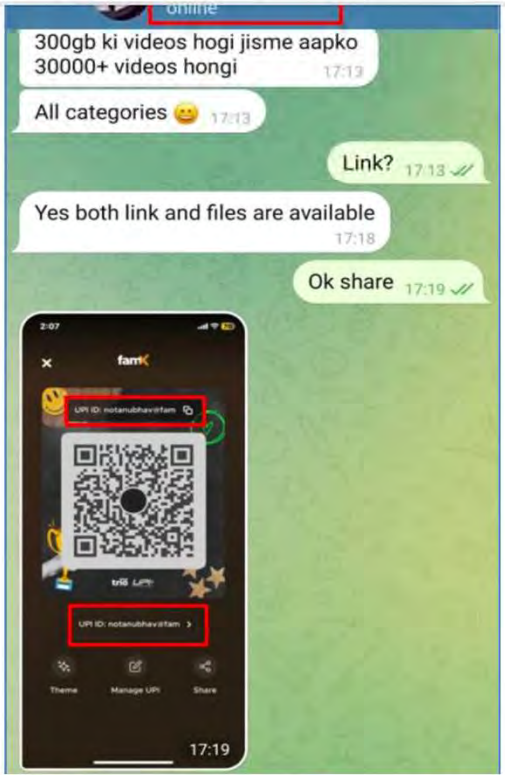
The public is urged to remain vigilant and immediately report any instance of child sexual exploitation or abuse material through the 1930 Cyber Helpline or the National Cybercrime Reporting Portal (www.cybercrime.gov.in).

Jharkhand Police remains committed to safeguarding children from online exploitation and ensuring strict action against perpetrators of such heinous crimes.

"Shockingly, the network extended internationally, with content being supplied to foreign citizens in Oman, Bangladesh, and UAE," the official added. PTI ANB MNB

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | [redacted] | JHARKHAND | This videos and photos of mine is posted without my permission by someone<br>Someone has shared this photos and videos screenshot with me from this website called hotpic.one<br>These are uploaded without my concern<br>Am getting lots of abusive message<br>Am getting sucidal thoughts<br>And also people are asking me for amount<br>This should be deleted immediately<br>From every website and shoul be banned | Sexually Obscene material | Registered | 23/05/2025 |




- I4C has identified a website **https://hotpic.one/** which is hosting Child Sexual Exploitative and Abuse Material (CSEAM), providing offenders a platform to upload, distribute, and circulate such contents. The platform acts as a digital marketplace where exploitative material is not only shared but also monetized, creating a disturbing cycle of exploitation.
- Further deep analysis reveals that the distribution of CSEAM extends beyond the website itself. Offenders are leveraging **Telegram channels** as secondary platforms to sell and disseminate CSEAM in a more organized manner by monetizing the same. It poses a threat to child safety. Hence, there is an urgent need for legal action on the same.

# PRACTICES IN STATES

## KERALA

- Counter child sexual exploitation center
- P HUNT operations & VIDTF
- Use of tools for CSEAM Identification across platforms

## TELANGANA

- More than 821 FIRs registered this year
- Use of specialised tools for cyber patrolling for CSEAM

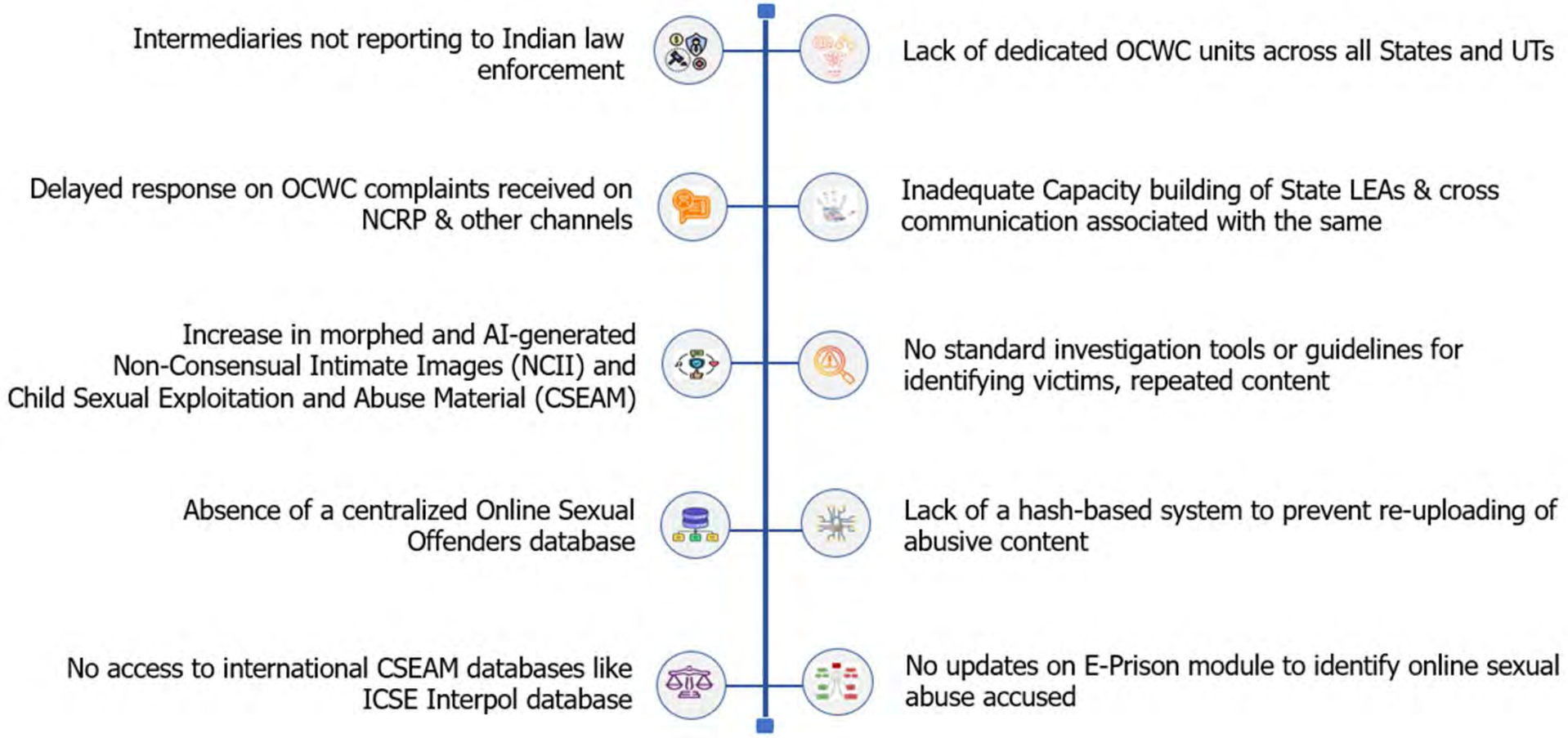
## Punjab

- Educated Teachers from 3,968 Government High Schools on their role to ensure the safety of school children in the digital space.


## DELHI

- Action against repeat offenders and content creators based on I4C Intel

# Current Challenges on Online Crimes against Women and Children



# PROPOSED ACTION PLAN

- **Setting up dedicated OCWC units at state HQ – Proposed sub Units**
- **Strengthen 1930 call centres** to accept OCWC complaints by dedicated, well trained personnel.
- **Role of Judicial wing:** Appraise the prosecution wings of such cases– and to appreciate the evidence in such matters – and to timely prosecute such cases – 63(4) BSA certificates – forensic medical board for age of child determination
- **Master Trainers –** Capacity building in a more focused approach to create a Task Force for operations and investigations **-Use of Forensic tools** and expertise for investigation.
- Focused **attention on timely blocking/take down** of content/data preservation/data request through Sahyog.
- **Section 28 of POCSO** - (3) The Special Court constituted under this Act, notwithstanding anything in the Information Technology Act, 2000 (21 of 2000)shall have jurisdiction to try offences under section 67B of that Act in so far as it relates to publication or transmission of sexually explicit material depicting children in any act, or conduct or manner or facilitates abuse of children online.

*****

# In a Landmark Verdict POCSO Court Sentences Two Child Predators to Death for Heinous Abuse of 33 Minor Children

Dated: 20.02.2026

The Court of the Special Judge, POCSO Cases, Banda, Uttar Pradesh, today, i.e., on 20.02.2026, has sentenced two accused namely, Rambhawan and his wife Durgawati to Death for the various offences under Indian Penal Code and POCSO Act including Unnatural Offences, Aggravated Penetrative Sexual Offences, Using Child for Pornographic Purposes, Storage of Pornographic Material involving Children, Abetment and Criminal Conspiracy.

The Ld. Trial Court also ordered for award of compensation of Rs. 10 Lakh to each victim by the Government. The Court further ordered to distribute the cash amount seized from the house of the accused persons among the victims in equal proportion.

The Central Bureau of Investigation (CBI) registered the case on 31.10.2020 against accused Rambhawan and other unknown persons on allegations of sexual abuse of children; using children for pornographic purposes; and creation and dissemination of Child Sexual Abuse Material over Internet.

During the investigation of the case, it surfaced that the accused persons had committed various nature of perversity including aggravated penetrative sexual assaults against 33 male children, some of them as young as three years of age. Investigation also revealed that some of the victims had suffered injuries on their private parts during penetrative sexual assault. Some of them have remained admitted in the hospital. Few of the victims developed Squint Eye. Victims are still suffering from psychological trauma caused by the predators. The predators remained active in the general area of Banda and Chitrakoot in Uttar Pradesh between Year 2010 to 2020. The accused Rambhawan was working as Junior Engineer in the Department of Irrigation. The accused used to apply different forms of modus operandi on children including access to online video-games and giving money/gifts to allure them.

CBI conducted a meticulous and thorough investigation in the case. The investigation remained sensitive towards the minor victims while conducting their examinations and ensured their emotional well-being through counselling. During the investigation, seamless coordination was ensured with forensic experts, medical experts dealing with child sexual abuse cases and child protection authorities. Investigation also ensured handling and preservation of digital evidence.

After conclusion of the investigation, CBI filed chargesheet on 10.02.2021 against the accused Rambhawan and his wife Durgawati. Charges were framed on 26.05.2023.

While awarding the severest punishment, the Ld. Court found the criminal acts of accused as "rarest of rare" on the basis of unparalleled depravity and systemic nature of their crimes, which involved the orchestrated sexual exploitation and abuse of 33 minor children. The sheer scale of this victimization across multiple districts, combined with the extreme moral turpitude of the convicts, marks this as a crime of such an exceptional and heinous nature that it leaves no room for reformation, necessitating the ultimate judicial deterrent to meet the ends of justice.

The CBI remains steadfast in its commitment to identifying, investigating, and prosecuting cases involving child sexual abuse and exploitation. The Bureau continues to accord top priority to such offences and reaffirms its resolve to safeguard the rights and dignity of children.

*****

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Indian Cyber Crime Coordination Centre
सहवीर्यं करवावहै • Working Together With Vigour

# THANK YOU


**Presented By:**

**Aishwarya Dongre, IPS**
**Online Crime Against Women and Children (OCWC)**
**Indian Cyber Crime Coordination Centre (I4C)**
**Ministry of Home Affairs**

**dd-i4c6@gov.in**