NEXT IAS

DAILY EDITORIAL ANALYSIS

TOPIC

DIGITAL CHILD ABUSE: DANGER OF AI-BASED EXPLOITATION

DIGITAL CHILD ABUSE: DANGER OF AI-BASED EXPLOITATION

Context

- Digital child abuse, fueled by AI-based exploitation, is an emerging threat, and protecting children from these dangers requires urgent regulatory, technological, and social interventions.

Digital Child Abuse & Implications

- Digital child abuse refers to **any form of harm** inflicted on children through online platforms. It includes:
    - **Cyberbullying:** Harassment and intimidation through social media, messaging apps, and gaming platforms.
    - **Exposure to Harmful Content:** Children being exposed to pornography, graphic violence, and inappropriate material.
    - **Online Grooming:** Predators luring minors into exploitative relationships.
    - **Child Sexual Abuse Material (CSAM):** It refers to material (audio, video, and images) that depicts a sexually explicit portrayal of a child.
    - **Identity Theft and Privacy Violations:** Misuse of children's personal data for illegal activities.
    - **Data Mining and Privacy Breaches:** AI algorithms analyze children's data from educational apps, social media, and gaming platforms to create behavioral profiles, which can be exploited by malicious actors for targeted manipulation, harassment, or identity theft.
- **International AI Safety Report 2025** flags the imminent risk of the generation, the possession, and the dissemination of CSAM with the help of AI tools.
- **Internet Watch Foundation**, in October 2024, underscored the proliferation of CSAM on the open web.
- The **World Economic Forum**, in 2023, highlighted how generative AI can create life-like images, especially of children.

Current Status Digital Child Abuse

- According to the **National Crime Records Bureau (NCRB) Report 2022**, cybercrimes against children have **substantially increased** compared to the previous year's statistics.
- Moreover, the **National Cyber Crime Reporting Portal (NCRP)**, under the aegis of the **Cyber Crime Prevention against Women and Children (CCPWC) scheme**, recorded 1.94 lakh child pornography incidents as of April 2024.
- In 2019, the NCRB signed a MoU with the National Centre for Missing and Exploited Children (NCMEC), USA to receive **tip-line reports on CSAM.**
    - As of March 2024, 69.05 lakh cyber tip-line reports have been shared with the States and Union Territories concerned.

Challenges in Addressing Digital Child Abuse

- **Lack of Robust Digital Laws:** While laws like the POCSO Act and IT Act exist, enforcement remains inconsistent, and legal loopholes allow perpetrators to evade justice.
    - The existing legislative framework lacks adequate safeguards to deal with the AI-generated CSAM.
- **Anonymous Nature of Cybercrime**: Offenders exploit encryption and the dark web to remain undetected.
- **Slow Legal Processes:** Convictions in cyber abuse cases are often delayed due to lack of technical expertise in law enforcement.
- **Rapid Growth of AI and Deepfake Technology:** Deepfake tools are being misused to manipulate images of children, further complicating efforts to combat exploitation.
- **Challenges in Reporting and Victim Support:** Victims and their families often hesitate to report due to social stigma, lack of trust in law enforcement, and fear of re-victimization.
- **Lack of Digital Literacy:** Many parents and teachers are unaware of online threats.

Government Measures and Legal Framework

- **Information Technology (IT) Act, 2000:** Criminalizes online child pornography, cyberstalking, and identity theft.

- ◆ **Section 67B of the IT Act 2000** punishes those who publish or transmit material in electronic form depicting children in sexually explicit acts.
- **Protection of Children from Sexual Offences (POCSO) Act, 2012:** Strengthened provisions to punish online child exploitation.
  - ◆ **Sections 13, 14, and 15 of the POCSO** prohibit using children for pornographic purposes, storing child pornography in any form, and using a child for sexual gratification.
- **Bharatiya Nyaya Sanhita (BNS): Section 294** of BNS penalises the sale, distribution, or public exhibition of obscene materials.
  - ◆ **Section 295** makes it illegal to sell, distribute, or exhibit such obscene objects to children.
- **National Cyber Crime Reporting Portal:** Enables citizens to report cases of cybercrime, including CSAM.
- **Collaboration with Social Media Companies:** The government works with platforms like Meta, Google, and WhatsApp to remove harmful content.
- **Awareness Campaigns:** Programs like the **Digital India** initiative promote safe internet usage for children.
  - ◆ The Press Information Bureau (PIB) has confirmed that the Indian government is actively working on measures to tackle online pornography and abuse.

Way Forward

- **Stronger AI-Based Detection Tools:** Automated systems to detect and remove CSAM quickly.
- **Cybersecurity Education:** Teaching children safe online habits.
- **Parental Controls and Monitoring:** Encouraging responsible digital parenting.
- **International Collaboration: International Cooperation**: Working with INTERPOL, EUROPOL, and UNICEF to track and prosecute offenders across borders.

Conclusion

- Digital child abuse is a pressing issue in India that requires urgent intervention. While the government has taken steps to counter online threats, technological advancements have also increased the risk of AI-based exploitation.
- A combination of stricter regulations, awareness, and advanced monitoring is essential to protect children in the digital world.

Source: TH

Mains Practice Question
[Q] What ethical and legal measures should be prioritized to combat the misuse of AI in creating exploitative content involving children, and how can society ensure the protection of vulnerable groups in the digital age?

■■■■