*Page: 2116-2145* *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

# LawFoyer International Journal of Doctrinal Legal Research

**[ISSN: 2583-7753]**

**Volume 3 | Issue 4**

**2025**

*DOI: https://doi.org/10.70183/lijdlr.2025.v03.215*

# PROTECTING DIGNITY IN CYBERSPACE: A CRITICAL ANALYSIS OF JUDICIAL RESPONSES TO DIGITAL SEXUAL EXPLOITATION IN INDIA

**Ankit Yadav**[1]

## I. ABSTRACT

*The advent of digital technologies has transformed communication and access to information, but it has also given rise to a disturbing increase in cyber-enabled crimes, disproportionately affecting women and children. Online sexual harassment, cyberbullying, image morphing, and the circulation of child sexual exploitative and abuse material (CSEAM) are becoming alarmingly widespread, often slipping through the cracks of traditional legal mechanisms. In response to these emerging harms, the Indian judiciary has assumed a crucial role in safeguarding constitutional values, particularly dignity, privacy, and personal security, within the digital sphere. This paper critically examines judicial responses in India to the growing threat of digital sexual exploitation, with particular reference to significant judicial interventions and landmark decisions, including Shreya Singhal v. Union of India, In Re: Prajwala Letter and Just Right for Children Alliance v. S. Harish, among others. These decisions collectively reflect the evolving approach of the judiciary towards enhancing platform accountability, compelling state action, and strengthening protections against online sexual abuse, especially in relation to the criminalisation, circulation, and consumption of CSEAM. Through judicial directions on content regulation, technological safeguards, and preventive mechanisms, courts have contributed to shaping a responsive legal framework aimed at victim protection and digital safety. Drawing on a doctrinal analysis of Articles 21 and 19(2) of the Indian Constitution, this study explores how the judiciary has sought to balance freedom of speech with the pressing necessity of curbing online sexual offences, particularly those involving CSEAM. It further evaluates the broader implications of judicial interventions on regulatory and institutional frameworks, positioning the Indian judiciary as a*

[1] Ph.D. (Law) - Research Scholar, University School of Law & Legal Studies (USLLS), Guru Gobind Singh Indraprastha University (GGSIPU), Delhi (India). Email: ankitlaw97@gmail.com

*pivotal force in fostering a safer, dignity-centered, and constitutionally compliant digital environment for women and children in India.*

## II. KEYWORDS

Cyber Crime, Child Pornography, Digital Exploitation, Online Sexual Harassment, Platform Accountability, etc.

## III. INTRODUCTION AND RESEARCH PROBLEM

In the present era of modernization and rapid technological advancement, the internet has emerged as one of the most transformative and indispensable tools for information dissemination, communication, and empowerment. It has effectively turned the world into a global village, offering a multitude of opportunities across diverse spheres, including online business, employment, advocacy, education, political mobilization, and social interaction. The internet has further enabled individuals to engage in meaningful conversations, express dissenting views, and participate in democratic discourse through platforms such as *'X'* (*formerly known as* Twitter), Facebook, Instagram, and various dating and discussion applications.

However, this rapidly expanding digital public sphere also harbours a darker and more troubling dimension. These platforms, while fostering open dialogue and participation, have increasingly become spaces of hostility, particularly for women, children, and other vulnerable groups. Online sexual harassment, abuse, trolling, cyberstalking, and technology-facilitated sexual violence have become pervasive, often resulting in the silencing of voices through intimidation and fear. Victims are frequently subjected to backlash, threats, reputational harm, and long-term psychological trauma, thereby undermining their dignity, autonomy, and right to safe participation in cyberspace.

India's social and legal systems have struggled to keep pace with the rapidly evolving landscape of cyber threats. While anonymity remains a cornerstone of digital privacy and free expression in democratic societies, the same anonymity has been systematically exploited by perpetrators to conceal their identities, evade accountability, and perpetuate

sexual exploitation online. This inherent duality of cyberspace significantly complicates the attribute of responsibility and enforcement of legal remedies, rendering traditional legal mechanisms increasingly inadequate.[2]

Digital Victimization defined as the experience of harm, harassment, or abuse through digital means is not a new phenomenon.[3] However, legal discourse has predominantly focused on defining cybercrime and improving technological mechanisms to detect perpetrators, rather than addressing the lived experiences of victims and the broader causes of their exploitation. This gap highlights the need for a rights-centric and victim-oriented legal approach.[4]

According to data released by the National Crime Records Bureau (NCRB) for the year 2023, cybercrimes against women continue to be a serious and growing concern in India. It is important to recognize that these reported figures are likely to represent only a portion of the actual problem, as it is estimated that nearly two-thirds of such cases go unreported due to factors such as fear of stigma, lack of awareness, or limited trust in law enforcement. The reported incidents encompass a wide range of offences, including blackmailing and threatening, cyber pornography, stalking, defamation, morphing, fake profiles, and other forms of digital abuse. The following table provides a detailed breakdown, including the top 5 states with the highest reported incidents:

[2] United States Department of Justice, Criminal Division, *Report on Online Child Exploitation Trends* (2023).
[3] United Nations Office on Drugs and Crime, *Cybercrime and Victimization: Challenges and Responses* (UNODC 2019).
[4] Susan W Brenner and Leo L Clarke, 'Distributed Security: Preventing Cybercrime' (2005) 23 *John Marshall Journal of Computer and Information Law* 659.

**Table 1: Cyber Crimes against Women - Top 5 States, India (NCRB 2023)**

| State/UT | Cyber Blackmailing/ Threatening | Cyber Pornography/ Hosting/ Publishing Obscene Sexual Materials | Cyber Stalking/ Cyber Bullying of Women | Defamation/ Morphing | Fake Profile | Other Crimes against Women | Total Cyber Crimes against Women |
|---|---|---|---|---|---|---|---|
| Karnataka | 0 | 457 | 4 | 1 | 0 | 6,540 | 7,002 |
| Maharashtra | 18 | 40 | 415 | 0 | 23 | 2,006 | 2,502 |
| Uttar Pradesh | 92 | 389 | 18 | 2 | 2 | 960 | 1,463 |
| Telangana | 38 | 78 | 295 | 2 | 2 | 1,032 | 1,447 |
| Tamil Nadu | 14 | 76 | 27 | 1 | 0 | 944 | 1,062 |
| Total *(All India)* | 304 | 2,767 | 1,358 | 505 | 102 | 14,474 | 19,510 |

*Source: NCRB Data on Cybercrimes against Women, 2023*

While digital victimization affects both men and women, studies and official statistics confirm that women are disproportionately targeted. The National Crime Records Bureau (NCRB) data for 2023 reveals a total of 19,510 reported cybercrimes against women, with the highest number of cases originating from Karnataka (7,002), followed

by Maharashtra (2,502), Uttar Pradesh (1,463), Telangana (1,447), and Tamil Nadu (1,062). The most commonly reported crimes include cyber pornography and publication of obscene material (2,767 cases), cyberstalking and bullying (1,358), and blackmailing or threatening (304). As per the data, Karnataka alone accounted for 6,540 cases under "*other crimes against women*", indicating broader, possibly under-classified offenses.[5]

These offenses frequently include cyberstalking, image morphing, creation and circulation of deepfake pornography, sexual threats, and online bullying, reflecting deep-rooted gender biases amplified through digital mediums.[6] Social media's open accessibility often becomes a weapon for sexualised and gendered attacks, with little immediate recourse for victims.

Children, too, have become increasingly vulnerable. The NCRB 2023 data reveals disturbing trends in cybercrimes against children, with cases recorded across India. It's worth noting that these figures might only reflect a portion of the reality, as a significant number of cases are believed to go unreported. The most common form of cybercrime against children is cyber pornography, followed by blackmailing and cyber stalking. The following table provides a detailed breakdown, including the top 5 states with the highest reported incidents:

[5] National Crime Records Bureau, *Crime in India 2023: Statistics Volume II* (Ministry of Home Affairs, Government of India, 2025) 831 https://www.ncrb.gov.in/uploads/files/2CrimeinIndia2023PartII2.pdf accessed 26 December 2025.

[6] ECPAT International and ECPAT Luxembourg, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (2016) 20.

**Table 2: Cyber Crimes against Children - Top 5 States, India (NCRB 2023)**

| State/UT | Cyber Blackmailing/ Threatening/ Harassment | Fake Profile | Cyber Pornography/ Hosting or Publishing Obscene Sexual Material depicting children | Cyber Stalking/ Bullying | Internet Crimes through Online Games etc. | Other Cyber Crimes against Childrn | Total Cyber Crimes against Childrn |
|---|---|---|---|---|---|---|---|
| Kerala | 0 | 0 | 342 | 3 | 0 | 98 | 443 |
| Karnataka | 0 | 0 | 341 | 0 | 0 | 22 | 363 |
| Rajasthan | 0 | 0 | 254 | 6 | 0 | 46 | 306 |
| Odisha | 0 | 0 | 69 | 0 | 0 | 0 | 69 |
| Madhya Pradesh | 0 | 0 | 5 | 5 | 0 | 33 | 43 |
| Total *(All India)* | 2 | 0 | 1,499 | 28 | 0 | 373 | 1,902 |

*Source: NCRB Data on Cybercrimes against Children, 2023*

The NCRB's 2023 data shows 1,902 total reported cases of cybercrimes against children, with the most prevalent offense being cyber pornography depicting children (1,499 cases). Kerala leads with 443 such incidents, followed by Karnataka (363), Rajasthan (306), Odisha (69), and Madhya Pradesh (43). These figures are alarming given the sensitive age

group and the long-term psychological and developmental damage such crimes can cause.[7] Moreover, other offences include cyberstalking/bullying (28 cases) and online blackmailing and harassment (2 cases), pointing to the multifaceted risks children face in digital spaces, including emerging and under-classified forms of online exploitation.

It is important to note that these figures may only represent a fraction of the actual problem, as estimates suggest that nearly two-thirds of cases go unreported, especially those involving women and children, due to fear of stigma, lack of digital literacy, or distrust in law enforcement systems.[8]

Moreover, during the COVID-19 pandemic, the shift to virtual modes of education, work, and socialization significantly increased online presence particularly for children and women thereby exacerbating their vulnerability. In India alone, with over 692 million internet users as of January 2023, approximately 30.4% were children, many of whom were exposed to heightened risks due to prolonged and unsupervised internet use.[9] Children, especially girls, became increasingly susceptible to grooming, child pornography, and sexual exploitation.[10]

Against this backdrop, a critical research problem emerges, while digital sexual exploitation has intensified in scale and complexity, the Indian legislative and executive responses have often remained fragmented and reactive. In this context, the judiciary has assumed an increasingly significant role in interpreting constitutional guarantees of dignity, privacy, and free expression, and in shaping normative standards for platform accountability and victim protection. This paper therefore examines how Indian courts

[7] National Crime Records Bureau, *Crime in India 2023: Statistics Volume II* (Ministry of Home Affairs, Government of India, 2025) 832 https://www.ncrb.gov.in/uploads/files/2CrimeinIndia2023PartII2.pdf accessed 26 December 2025.

[8] Sonia Livingstone, John Carr and Jasmina Byrne, *One in Three: Internet Governance and Children's Rights* (UNICEF Office of Research-Innocenti, 2016) https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html accessed 28 December 2025.

[9] Simon Kemp, *Digital 2023: India* (Datareportal, January 2023) https://datareportal.com/reports/digital-2023-india accessed 20 December 2025.

[10] ET Now Digital, 'COVID-19 Lockdown Sees a Surge in Online Child Sexual Abuse Cases', *Times Now* (22 April 2021) https://www.timesnownews.com/mirror-now/in-focus/article/covid-19-lockdown-sees-a-surge-in-online-child -sexual-abuse-cases/744764 accessed 20 December 2025.

have responded to the challenge of digital sexual exploitation, and whether judicial interventions have been effective in bridging regulatory gaps, balancing competing rights, and ensuring a dignity-centred and rights-based framework for protecting women and children in cyberspace.

### A. Research Questions

Digital technologies have greatly expanded avenues for communication and information sharing, but they have also facilitated new forms of sexual exploitation, disproportionately affecting women and children. In the context of fragmented legislative and executive responses, the judiciary has become a crucial actor in protecting victims, ensuring platform accountability, and upholding constitutional rights. In light of this, the study seeks to examine the following specific research questions:

1. How have Indian courts addressed digital sexual exploitation to protect dignity, privacy, and free expression?
2. How effective are judicial interventions in bridging regulatory gaps and safeguarding women and children?

### B. Research Methodology

This study adopts a doctrinal and analytical research methodology to examine the legal, institutional, and judicial responses to digital sexual exploitation of women and children in India. It relies on primary sources such as statutes, rules, and government regulations, and secondary sources including reports, scholarly articles, and policy documents on cybercrime, digital victimization, and child protection.

The research employs a qualitative approach, interpreting constitutional provisions, laws, and judicial reasoning to evaluate the effectiveness of legal frameworks and institutional measures. The methodology focuses on understanding how courts and authorities balance fundamental rights, ensure platform accountability, and develop a rights- and dignity-centered framework for safeguarding vulnerable groups in cyberspace.

### C. Literature Review

Digital sexual exploitation has emerged as a serious threat to dignity in cyberspace, disproportionately impacting women and children. Sonia Livingstone, John Carr and Jasmina Byrne in One in Three: Internet Governance and Children's Rights (2016)[11] and Simon Kemp in Digital 2023: India (2023)[12] highlight that online harassment, cyberstalking, image-based sexual abuse (IBSA), and non-consensual dissemination of intimate content are deeply gendered harms rooted in patriarchal power relations and amplified by digital platforms.

These practices extend beyond traditional notions of "revenge porn" to include sextortion, voyeurism, and deepfake-enabled exploitation, resulting in serious violations of privacy, autonomy, and human dignity.

The scale of digital sexual exploitation is reflected in official crime statistics. The Crime in India 2023: Volume II (2025) published by National Crime Records Bureau recorded 19,510 cybercrime cases against women and 1,902 cases against children, involving cyber pornography, stalking, blackmail, and circulation of CSAEM.[13] Some scholars argued that existing legal responses remain fragmented and reactive, failing to address the structural and technological enablers of such abuse.

Reports such as Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse by ECPAT International and ECPAT Luxembourg (2016) emphasize the need for survivor-centered, rights-based frameworks that integrate prevention, accountability, and institutional support to protect dignity in digital spaces.[14]

---

[11] Sonia Livingstone, John Carr and Jasmina Byrne, *One in Three: Internet Governance and Children's Rights* (UNICEF Office of Research-Innocenti, 2016) https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html accessed 28 December 2025.
[12] Simon Kemp, *Digital 2023: India* (Datareportal, January 2023) https://datareportal.com/reports/digital-2023-india accessed 20 December 2025.
[13] National Crime Records Bureau, *Crime in India 2023: Statistics Volume II* (Ministry of Home Affairs, Government of India, 2025) 832 https://www.ncrb.gov.in/uploads/files/2CrimeinIndia2023PartII2.pdf accessed 26 December 2025.
[14] ECPAT International and ECPAT Luxembourg, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (2016) 20.

Within the Indian legal discourse, Akanksha Pathak and Prateek Tripathi, in Digital Victimization of Women in Cyberspace: An Analysis of Effectiveness of Indian Cyber Laws (2023), critically examine how cyber abuse against women represents an extension of offline gender inequality into online environments.[15] The authors argue that technological anonymity, evidentiary challenges, and offence-centric regulation under the Information Technology Act, 2000 undermine effective judicial protection of dignity and privacy. Despite constitutional guarantees under Articles 14 and 21, low conviction rates and limited victim-centric remedies reveal significant gaps in judicial and institutional responses to digital sexual exploitation.

The judicial and regulatory challenges are further intensified in cases involving children and emerging technologies. Online Safety for Children: Protecting the Next Generation from Harm (2023) documents how early digital exposure increases children's vulnerability to grooming, privacy violations, and CSAEM.[16] These concerns are amplified in Digital Child Abuse, the Danger of AI-Based Exploitation by Shivang Tripathi and Neha Singh (2025), which warns that generative AI enables the creation of hyper-realistic CSAEM, blurring the distinction between real and synthetic harm.[17] The authors contend that Indian statutes such as the IT Act, 2000 and the POCSO Act are ill equipped to address AI-driven exploitation, highlighting the need for proactive judicial interpretation and technology-responsive reforms to uphold dignity in cyberspace.

## IV. LEGAL FRAMEWORK FOR DIGITAL PROTECTION OF WOMEN AND CHILDREN

[15] Akanksha Pathak and Prateek Tripathi, 'Digital Victimization of Women in Cyberspace: An Analysis of Effectiveness of Indian Cyber Laws' (2023).
[16] *Online Safety for Children: Protecting the Next Generation from Harm* (NITI Aayog, Government of India 2023) http://niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-fromharm.pdf accessed 26 December 2025.
[17] Shivang Tripathi and Neha Singh, 'Digital Child Abuse, the Danger of AI-Based Exploitation' *The Hindu* (3 April 2025).

### A. International Legal Framework for Digital Protection of Women and Children

The international legal framework for the protection of women against violence both offline and online has evolved to respond to the growing challenges of the digital age. The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979, serves as a cornerstone in this regard.[18] Referred to as the International Bill of Rights for Women, the Convention obligates State parties to eliminate discrimination in all its manifestations. Article 1 defines discrimination as "any distinction, exclusion or restriction made on the basis of sex" that impairs or nullifies women's rights and fundamental freedoms. Article 2 further compels States to undertake "appropriate legislative and other measures" to prohibit and prevent such discrimination. These provisions, though enacted in a pre-digital context, are increasingly interpreted to encompass online spaces where women frequently face gendered cyber violence including online abuse, cyberstalking, doxing, and the non-consensual dissemination of intimate content.

The UN Declaration on the Elimination of Violence against Women, 1993, further contextualizes the nature of harm. It recognizes that violence against women encompasses "physical, sexual and psychological harm or suffering," including that occurring in private or public spheres.[19] The Preamble and Article 1 of the Declaration acknowledge that technological advancements have facilitated new forms of violence. Acts such as online harassment and image-based sexual abuse now fall within the scope of such violence, warranting a legal response that is both robust and adaptive. Complementing these instruments is the Beijing Declaration and Platform for Action, 1995, which highlights the need for States to adopt specific legal, policy, and educational measures to combat gender-based violence perpetrated through information and communication technologies. It calls upon States to strengthen access to justice, foster

[18] The Convention on the Elimination of All Forms of Discrimination Against Women, 18 December 1979, 1249 UNTS 13.
[19] Declaration on the Elimination of Violence Against Women, GA Res 48/104, UN GAOR, 48th Sess, Supp No 49, UN Doc A/RES/48/104 (20 December 1993).

digital literacy among women, and ensure safe online environments through legislative safeguards.[20]

In parallel, the Budapest Convention on Cybercrime, 2001, the first and most significant international treaty addressing crimes committed via computer networks offers a procedural and substantive legal framework to counter cyber-enabled offences.[21] Although not gender-specific, the Convention is instrumental in combating crimes that disproportionately affect women and children. Article 9 mandates State parties to criminalize the "production, offering, distribution, procurement, or possession" of child pornography, including when such material is disseminated electronically. Its procedural provisions, encapsulated in Articles 14 to 21, provide States with legal tools to secure electronic evidence, conduct expeditious investigations, and cooperate across borders. These measures are crucial for ensuring that digital platforms do not become safe havens for perpetrators and that justice mechanisms remain effective in the face of evolving technological abuse.[22]

These international instruments not only delineate the legal obligations of States but also reflect a shared human commitment: to ensure that women and children, irrespective of geography, live free from fear, violence, and exploitation, both offline and online. The recognition of digital harms within traditional human rights frameworks highlights the importance of treating online safety as an extension of fundamental human dignity.

### B. National Legal Framework for Digital Protection of Women and Children

In response to the growing incidence of cybercrimes targeting women and children, India has enacted a range of legislative measures. The Information Technology Act, 2000 (amended in 2008) forms the bedrock of India's cyber law framework, criminalizing offenses such as cyberstalking, identity theft, publishing obscene material in electronic

[20] The Beijing Declaration and Platform for Action, UN Fourth World Conference on Women, UN Doc A/CONF.177/20 (15 September 1995).
[21] The Council of Europe, Budapest Convention on Cybercrime, ETS No 185 (23 November 2001).
[22] Ibid.

form (Section 67), and transmitting sexually explicit content (Section 67A and 67B), including material involving children. However, these provisions are general and not victim-specific, leaving gaps in redressal mechanisms for women and children.[23]

While the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 regulate how sensitive personal data should be protected, they fall short of providing legal remedies against online violence or harassment. India urgently requires a specialized cyber law addressing gender-based and child-specific online crimes, aligned with international obligations under instruments such as the Budapest Convention on Cybercrime and supported by integrated enforcement and judicial mechanisms.[24]

To address child-specific offenses, the Protection of Children from Sexual Offences (POCSO) Act, 2012 criminalizes offenses including child pornography, online grooming, and cyber-enabled sexual abuse.[25] Nevertheless, it does not extend explicit protections to adult women. The Indian Penal Code, 1860 provides penalties for crimes such as rape (Section 375), voyeurism (Section 354C), stalking (Section 354D), and criminal intimidation (Section 506), but these provisions are largely offline-centric and reactive rather than preventive in the digital realm.[26]

Complementary laws include the Indecent Representation of Women (Prohibition) Act, 1986 -expanded through the 2018 amendment to include digital platforms - and the Protection of Women from Sexual Harassment at Workplace Act, 2013, which increasingly intersects with cyber-harassment in professional settings.[27] The Digital Personal Data Protection Act, 2023 now plays a crucial role in safeguarding the privacy

[23] The Information Technology Act, 2000.
[24] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), 2011.
[25] The Protection of Children from Sexual Offences (POCSO) Act, 2012.
[26] The Indian Penal Code, 1860.
[27] The Protection of Women from Sexual Harassment at Workplace Act, 2013.

of personal data, including that of women and children, by establishing lawful grounds for data processing and penalties for breach.[28]

Recent legislative developments reflect a growing awareness. The Bharatiya Nyaya Sanhita, 2023 (BNS) recognises electronic and digital records within the definition of "documents" (Section 2(8)) and addresses cyberstalking against women under Section 78. Yet, various cyber offences are omitted or insufficiently articulated, and Section 111, while referencing cybercrimes, fails to prescribe punishment proportionate to their severity.[29]

Likewise, the Bharatiya Sakshya Adhiniyam, 2023 (BSA) addresses digital evidence, notably through Section 2(vi) (definition of electronic records) and Sections 39–40, which allow expert testimony on technological evidence.[30] However, it too lacks comprehensive procedural norms specific to the preservation and admissibility of digital evidence in cybercrime cases involving vulnerable groups.

Despite these efforts, there exists no singular, consolidated legal framework in India specifically addressing online crimes against women and children. Agencies are fragmented, and implementation mechanisms are disjointed. Recognizing this gap, states like Rajasthan have initiated model drafts aimed at developing a dedicated law addressing online sexual exploitation, cyber harassment, revenge pornography, and child sexual abuse material (CSAM). The draft law also proposes victim-centered approaches, incorporating international best practices and addressing the unique vulnerabilities of digital victims.

In light of the complex, evolving nature of online offences, especially those disproportionately impacting women and children, there is an urgent need for a dedicated, gender- and child-sensitive cybercrime law.

[28] The Digital Personal Data Protection Act, 2023.
[29] The Bharatiya Nyaya Sanhita, 2023.
[30] The Bharatiya Sakshya Adhiniyam, 2023.

## V. INSTITUTIONAL AND POLICY RESPONSES TO COMBAT CHILD SEXUAL ABUSE MATERIAL (CSAM)

In September 2018, the Ministry of Home Affairs (MHA) established a nationwide cybercrime reporting platform under the Cybercrime Prevention against Women and Children (CCPWC) Scheme, enabling citizens to report offences related to child pornography and other online crimes through a dedicated online portal. This initiative was intended to enhance access to justice and to facilitate prompt reporting and investigation of such offences, particularly those involving Child Sexual Abuse Material (CSAM).

To strengthen the monitoring mechanism, the Indian government restricts access to websites hosting CSAM based on INTERPOL's "Worst-of List," which is regularly updated and enforced through the Central Bureau of Investigation (CBI) India's National Nodal Agency for INTERPOL coordination. The CBI, in collaboration with other law enforcement bodies, ensures the prompt removal and blocking of such content from the Indian internet ecosystem.

Further policy advancement occurred with the Ad Hoc Committee of the Rajya Sabha on the Alarming Issue of Pornography on social media and Its Effect on Children and Society, chaired by Hon'ble Shri M. Venkaiah Naidu in 2020.[31] The Committee made 40 comprehensive recommendations aimed at curbing the spread of CSAM and strengthening protective frameworks for children. Some of the important recommendations are:

1. Broadening the definition of child pornography, encompassing digitally altered content and emerging technologies.
2. Restricting children's access to pornographic material through mandatory parental controls and content classification protocols.

[31] Press Information Bureau, 'Cyber Crime Prevention against Women and Children Scheme, PIB (25 January 2020)' https://pib.gov.in/PressReleseDetailm.aspx?PRID=1600505 accessed 28 December 2025.

3. Imposing liability on Internet Service Providers (ISPs), social media platforms, and other intermediaries to prevent access to and ensure swift removal of CSAM.
4. Enhancing punitive measures under relevant laws such as the Protection of Children from Sexual Offences (POCSO) Act, 2012, and the Information Technology Act, 2000 for non-compliance with content regulation obligations.

In a significant operational move, the CBI launched "Operation Megh Chakra" in September 2022, a nationwide crackdown on the dissemination and sharing of CSAM.[32] The operation was initiated following intelligence received from INTERPOL's Singapore unit, highlighting the circulation of exploitative material via online platforms. The operation involved searches across multiple states and targeted suspects involved in the distribution of CSAM, with a focus on identifying both consumers and creators of such content.

The CBI also plays a pivotal role as India's liaison for INTERPOL's International Child Sexual Exploitation (ICSE) database. This globally integrated system contains images and videos related to child sexual abuse and is used by specialised law enforcement officers to identify victims, track offenders, and facilitate international collaboration in investigative processes.

These institutional and operational measures mark significant progress in India's evolving framework to tackle digital crimes against children. However, the growing sophistication of cyber offenders necessitates continuous updating of laws, advanced forensic capabilities, and enhanced inter-agency and international cooperation to ensure robust child protection in the digital age.

## VI. ROLE OF JUDICIARY IN ADDRESSING THE DIGITAL EXPLOITATION OF WOMEN AND CHILDREN

[32] Central Bureau of Investigation, 'CBI Today Conducts National Wide Searches in Meticulous Operation in Megh Chakra at Around 59 Locations in 21 States/UT etc. in Two Cases Related to Download/Circulation of CSAM (Sept 24, 2022)' https://cbi.gov.in/press-detail/NTI2Ng== accessed 28 December 2025.

The Indian Courts, in many landmark judgments, have provided necessary directions for safeguarding minors against sexual exploitation, particularly in cyberspace.

In Maria Kuttubudin Lokhandwala v. State of Maharashtra & Anr., the Bombay High Court laid down several precautionary measures to protect children from online sexual abuse. The Court directed the government to block pornographic websites, enforce strict regulations in cyber cafés to prevent children from accessing inappropriate content, and ensure that no unsuitable material is distributed or made available at such public access points.[33] These directions aimed to shield minors from the dangers of digital exposure and to strengthen institutional responsibility in curbing child sexual exploitation.

In Avinash Bajaj v. State (N.C.T. of Delhi), the Delhi High Court highlighted the legislative gaps in India's legal framework for addressing issues related to online pornography and internet regulation.[34] The Court observed that the existing Indian law was inadequate to tackle the rising problem of internet-based dissemination of sexually explicit material. Referring to international best practices, the Court noted that in the United States, legislation such as the Communications Decency Act, 1996, the Child Online Protection Act, 1998, and the Children's Internet Protection Act, 2003, have been enacted to prevent minors from accessing harmful online content. These Acts aim to restrict the communication or display of any obscene material depicting sexual or excretory activities to individuals under the age of 18 through interactive computer services.

In *Court on its own motion v. State of Punjab*, (2013) 3 RCR, the Court highlighted the importance of proper enforcement of the *Protection of Children from Sexual Offences Act, 2012* (POCSO Act), which aims to protect children from sexual abuse, violence, harassment, and pornography. The Court emphasized that the National Commission and State Commissions are designated as the authorities responsible for monitoring compliance under the Act. The *POCSO Act* includes the *Rules of 2012*, with Rule 6

[33] *Maria Kuttubudin Lokhandwala v. State of Maharashtra* (2020) 1 BOMCR 210 (Bom).
[34] *Avinash Bajaj v. State (N.C.T. of Delhi)* (2005) 116 DLT 427 (Del).

specifically outlining the monitoring responsibilities of these commissions, assigning them certain powers to ensure the Act's effective implementation. The Court stressed that these bodies must begin carrying out their responsibilities under the legislation to ensure the protection of children from sexual offences.[35]

In S. Harish v. Inspector of Police, the Madras High Court quashed the judicial proceedings and held that downloading child pornography is not an offence under Section 67B of the Information Technology (IT) Act, 2000. The Court ruled that viewing child pornography in itself did not constitute an offence, highlighting the legal intricacies surrounding the offence of child pornography and its classification under Indian law. This ruling reflected concerns over the legal gaps in regulating such crimes effectively.[36]

However, on 23 September 2024 the Hon'ble Supreme Court through a Division Bench comprising Chief Justice D.Y. Chandrachud and Justice J.B. Pardiwala, overturned this decision in Just Rights for Children Alliance v. S. Harish and adopted a purposive, dignity-centric interpretation of the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000 to address the digital sexual exploitation of children. The Court categorically held that the mere viewing of child sexual exploitation and abuse material (CSAEM), coupled with a failure to delete, destroy, or report it, constitutes an offence under Section 15(1) of the POCSO Act and is punishable even without proof of transmission or publication. Recognising such conduct as an "inchoate offence", the Court emphasised that possession includes constructive possession exercised through digital devices under one's control, thereby preventing offenders from evading liability through technical defences. Importantly, the Court observed that the commonly used expression "child pornography" or CSAM trivialises the harm suffered by victims and therefore directed the use of the term "child sexual exploitation and abuse material (CSAEM)" to accurately reflect the exploitative and abusive nature of the offence. The Court further permitted invocation of the statutory

[35] *Court on its own motion v. State of Punjab* (2013) 3 RCR.
[36] *S. Harish v. Inspector of Police,* (Crl. OP. 16056/2023).

presumption of culpable mental state under Section 30 of the POCSO Act even at the stage of quashing proceedings, reinforcing that judicial restraint at the threshold would defeat legislative intent and dilute constitutional protection of children's dignity.[37]

In Shreya Singhal v. Union of India, the Supreme Court struck down Section 66A of the Information Technology Act, 2000, as unconstitutional, affirming the primacy of the right to free speech and expression on digital platforms. While the case mainly dealt with issues of free expression, the Court also emphasized the need to protect individuals from online harassment and abuse, including the circulation of unsolicited obscene material. The Court interpreted Section 79(3)(b) of the Information Technology Act, 2000, concerning intermediary liability. The Court held that an intermediary (i.e., Internet Service Providers or ISPs) could only be compelled to remove or disable access to unlawful content upon receiving actual knowledge of the content being illegal or a court order. This judgment highlighted the limitations of ISPs in preventing or controlling illegal content unless formally notified by the government or a court ruling.[38]

In Kamlesh Vaswani v. Union of India & Others (2013) WP (C) 177, the Court focused on child pornography on the internet, particularly concerning websites displaying child pornography of minors between the ages of 14 and 18. The Court emphasized the urgency of addressing this growing issue and ordered that proactive measures should be taken by the relevant authorities to combat child pornography. Further instructions were issued to the Secretary of the Department of Transportation to file an affidavit clarifying whether government departments could issue directives to block such websites.[39]

In Mrs. X v. Union of India & Ors., the Delhi High Court directed the police to remove content that had been unlawfully uploaded on a pornographic website. The Court also ordered search engines to de-index the content from their results and instructed all concerned parties to implement preventive measures against the future dissemination of

[37] *Just Rights for Children Alliance v. S. Harish* 2024 INSC 716.
[38] *Shreya Singhal v. Union of India* (2015) SC 1523.
[39] *Kamlesh Vaswani v. Union of India & Others* (2013) WP (C) 177.

similar content. It emphasized the urgent need for effective remedial mechanisms for affected individuals and highlighted the importance of balancing the responsibilities of internet intermediaries with the rights of users. Further, the Court laid out the types of directions that courts can issue in such matters.[40]

In Ritesh Sinha v. State of Uttar Pradesh, the Allahabad High Court addressed a sextortion case in which the accused had obtained explicit photographs of the victim and subsequently used them for blackmail. The Court emphasized that such acts violate an individual's right to privacy and dignity and held the accused liable under several provisions including extortion and criminal intimidation.[41]

In Rupan Deol Bajaj v. Kanwar Pal Singh Gill, the Supreme Court recognised that stalking, whether conducted in person or through online means, constitutes a serious offence that violates an individual's right to privacy and causes psychological harm. The Court emphasised the necessity of implementing stringent legal measures to protect individuals from such intrusive conduct.[42]

In State of Kerala v. Rahul Pasupalan & Another, the Kerala High Court dealt with another sextortion case where the accused had circulated explicit videos of a woman without her consent. The Court acknowledged the serious nature of the offence and convicted the accused under various sections of the Indian Penal Code (IPC), including those related to voyeurism and defamation.[43]

In the landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court unequivocally recognized the right to privacy as a fundamental right under Article 21 of the Constitution. While primarily focused on the broader scope of privacy, the ruling acknowledged that the non-consensual dissemination of private images or videos commonly known as revenge pornography represents a severe infringement on personal

[40] *Mrs. X v. Union of India & Others* 2023 DHC 2806.
[41] *Ritesh Sinha v. State of Uttar Pradesh* AIR 2019 SC 3592.
[42] *Rupan Deol Bajaj v. Kanwar Pal Singh Gill* 1996 AIR 309.
[43] *State of Kerala v. Rahul Pasupalan & Another* Crime No. 2242 of 2020 of Kadakkavoor Police Station.

dignity and autonomy. The Court asserted that such unauthorized sharing of intimate content causes reputational harm, emotional trauma, and a breach of human dignity, thereby necessitating stringent legal protections.[44]

In Re: Prajwala Letter case, the Supreme Court of India considered the growing concern of child sexual abuse material (CSAM) being circulated over the internet. The case was filed by the NGO Prajwala, which urged the Court to direct the government to take appropriate action to prevent the spread of such content online. The Court issued several important directives, including the establishment of a centralised online portal for reporting CSAM, which would enable prompt removal of such material in coordination with internet service providers. The Court also directed the creation of specialised cybercrime cells in all states and union territories to deal with complaints related to CSAM. By recognising the complexity of cyber offences, the Court stressed the need for providing training to law enforcement officials to effectively address such crimes. It further highlighted the cross-border nature of CSAM and called for international cooperation through mutual legal assistance treaties and similar frameworks. The Court also directed the government to conduct awareness campaigns to educate the public about the dangers and consequences of CSAM. These directives, along with recommendations from a Supreme Court-appointed expert committee, ultimately informed the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, marking a significant step in India's efforts to curb online sexual exploitation and protect the rights and dignity of victims.[45]

In Ajay Goswami v. Union of India, the Supreme Court deliberated on the issue of transmitting indecent messages through electronic communication. It held that sending lewd or obscene content via emails, SMS, or other digital platforms attracts legal

[44] *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
[45] *In Re: Prajwala Letter Dated 18.02.2015 Videos of Sexual Violence and Recommendations* SMW (Crl.) No. 3/2015.

consequences under the Indian Penal Code. The Court affirmed that freedom of speech and expression does not extend to content deemed obscene or offensive.[46]

In Shafhi Mohammad v. State of Himachal Pradesh, the Supreme Court considered issues related to privacy and the admissibility of electronic evidence, particularly sexually explicit videos. The Court held that unauthorized dissemination of intimate content constitutes a violation of an individual's right to privacy and emphasized that electronic evidence must be handled with due regard to constitutional protections.[47]

In Yogesh Prabhu v. State of Maharashtra, the accused was held liable for cyber-stalking after persistently harassing a woman who had rejected his advances, despite previously engaging in amicable conversations. The matter was reported to the cyber cell, and the accused was convicted under Section 509 of the Indian Penal Code read with Section 66E of the Information Technology Act.[48]

In State of Tamil Nadu v. Suhas Katti, the accused disseminated derogatory and indecent messages through Yahoo Messenger groups and emails, using a fake email ID created in the name of the complainant. These actions led to reputational harm and abusive calls directed at the complainant. The court found the accused guilty under Sections 469 and 509 of the IPC and Section 67 of the Information Technology Act, 2000.[49]

In Shamsher Singh Verma v. State of Haryana, the issue before the Supreme Court was the admissibility of a Compact Disc submitted as evidence. The High Court had denied its exhibition, but the Supreme Court held that a Compact Disc qualifies as a document and is admissible. It clarified that Section 294(1) of the CrPC does not mandate personal admission or denial by the parties involved for the document to be considered.[50]

In State v. Jayanta Das, the Orissa High Court convicted the accused, a first-time offender, for cyber offences and emphasised the need to recognise the gravity of criminal intent.

[46] *Ajay Goswami v. Union of India* 2006 INSC 995.
[47] *Shafhi Mohammad v. State of Himachal Pradesh* (2018) 2 SCC 801.
[48] *Yogesh Prabhu v. State of Maharashtra* Case No. 3700686/PS/2009.
[49] *State of Tamil Nadu v. Suhas Katti* Case No. 4680 of 2004.
[50] *Shamsher Singh Verma v. State of Haryana* (2016) 15 SCC 485.

The Court observed that women's vulnerability in cyberspace is a pressing concern and that judicial intervention is essential to ensure their protection and access to justice.[51]

## VII. ANALYTICAL ENGAGEMENT WITH RESEARCH QUESTIONS: REFRAMING DIGNITY AND SAFETY IN THE DIGITAL AGE

### A. Judicial Approach in Protecting Women and Children

In response to the first question, Indian courts have increasingly recognized digital sexual exploitation as an extension of offline gendered inequalities, demanding interpretations of existing laws that prioritize dignity, privacy, and victim protection. In Just Rights for Children Alliance v. S. Harish (2024), the Supreme Court adopted a dignity-centric, inchoate offence approach, holding that possession, failure to delete, or neglect to report child sexual exploitation and abuse material (CSAEM) constitutes punishable conduct.[52] This judgment reflects a proactive judicial stance, emphasizing that offenders cannot evade liability through technicalities and that digital possession through devices falls within the ambit of statutory protection under the POCSO Act.

Courts have also emphasized institutional and preventive mechanisms to safeguard vulnerable groups. In Re: Prajwala Letter case (2015) the Court in the order dated 01st August 2023 directed the establishment of centralized reporting portals, specialized cybercrime cells, and coordination with intermediaries to ensure timely removal of exploitative material.[53] These measures demonstrate a holistic approach, combining legal interpretation with operational frameworks that extend protection beyond individual adjudication. By mandating reporting mechanisms and institutional oversight, the judiciary has sought to create a proactive system capable of addressing both immediate harm and recurring patterns of abuse in digital spaces.

---

[51] *State v. Jayanta Das* G.R. Case No.1739/2012.
[52] *Just Rights for Children Alliance v. S. Harish* 2024 INSC 716.
[53] *In Re: Prajwala Letter Dated 18.02.2015 Videos of Sexual Violence and Recommendations* SMW (Crl.) No. 3/2015.

Despite these advances, emerging technological threats pose new challenges. Generative AI, deepfakes, and hyper-realistic digital content can produce and circulate exploitative material with unprecedented speed, complicating enforcement and victim protection. Judicial strategies, while robust, now require integration with forward-looking legislation, technological safeguards, and preventive policy frameworks to ensure that dignity, privacy, and autonomy remain protected in rapidly evolving digital environments.

**B. Judicial Interventions in Safeguarding Women and Children**

With respect to the second question, Courts have played a crucial role in clarifying the scope of rights and legal protections online, particularly for privacy and freedom of expression. The Supreme Court in K.S. Puttaswamy (Retd.) v. Union of India affirmed the fundamental right to privacy under Article 21, establishing that unauthorized dissemination of private information, including intimate content, constitutes a serious infringement of personal dignity.[54] Similarly, in Shreya Singhal v. Union of India, the Court struck down Section 66A of the IT Act as unconstitutional while clarifying intermediary liability under Section 79.[55] These steps reflect the judiciary's effort to balance protection against harm with freedom of speech, setting a foundational framework for safeguarding digital rights.

Courts have further strengthened institutional and procedural mechanisms to bridge gaps in fragmented cyber regulations. By interpreting statutes purposively and issuing proactive directions, the courts have enhanced enforcement and accountability, particularly for vulnerable groups like women and children. For instance, the case of Just Rights for Children Alliance v. S. Harish (2024), expanded liability under the POCSO Act to cover digital possession and inaction[56], while In Re: Prajwala Letter case (2015) strengthened institutional responses by establishing centralized reporting, cybercrime

[54] *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
[55] *Shreya Singhal v. Union of India* (2015) SC 1523.
[56] *Just Rights for Children Alliance v. S. Harish* 2024 INSC 716.

cells, and inter-agency coordination.[57] Such interventions demonstrate a dual strategy: legal interpretation ensures statutory applicability, while institutional directives operationalize protective mechanisms. These steps reflect a recognition that the judiciary must not only interpret laws but also guide implementation to ensure consistent protection across cyberspace.

Nevertheless, rapid technological advancement and legislative gaps limit the full effectiveness of judicial measures. Deepfakes, AI-generated intimate content, and automated dissemination create complex evidentiary and enforcement challenges, while overlapping statutes and fragmented agencies hinder scalable protections. While judicial interventions are critical in shaping norms, sustained safety requires proactive legislation, advanced forensic capabilities, and digital literacy initiatives, complementing court-led guidance to bridge the divide between legal intent and evolving technological threats.

## VIII. SUGGESTIONS AND WAY FORWARD

The evolving nature of digital sexual exploitation demands responses that go beyond reactive legal measures. While judicial interventions play a crucial role, sustainable protection of women and children requires preventive, victim-centric, and education-driven reforms. Addressing institutional sensitivity, enforcement culture, and digital awareness can significantly strengthen the existing regulatory framework. The following suggestions aim to bridge these gaps through focused and practical interventions:

1. The early introduction of digital safety education as a compulsory subject in schools and colleges can help children and adolescents recognise online threats, understand the importance of consent and privacy, and equip them with preventive knowledge and responsible online behavior from an early age.

[57] *In Re: Prajwala Letter Dated 18.02.2015 Videos of Sexual Violence and Recommendations* SMW (Crl.) No. 3/2015.

2. The legal and institutional responses should adopt a victim-centric and trauma-informed approach that prioritizes dignity, confidentiality, and psychological well-being, reducing the risk of secondary victimization
3. The administrative and educational institutions must treat digital exploitation and harassment as serious misconduct, ensuring that complaints are addressed with swift, proportionate, and protective measures rather than minimal or symbolic actions, to safeguard victim safety and trust.
4. The persistence of online harassment, even after police intervention, indicates that legal measures alone are insufficient. There is a need for coordinated follow-up, continuous monitoring of reported cases, and sustained support mechanisms to ensure that victims are protected and offenders are held accountable.
5. The law enforcement agencies and cyber cells should be trained in trauma-informed and empathetic engagement with victims. Victim-friendly and accessible policing practices can encourage reporting, reduce fear and stigma, and ensure that victims feel supported throughout the investigation process.
6. The police and cyber cells should receive mandatory training in digital forensics, including the identification, collection, and preservation of electronic evidence. Specialized cyber experts are essential to ensure that digital crimes are investigated effectively and that evidence is admissible and robust for prosecution.
7. The legislative and regulatory frameworks must be regularly updated to keep pace with technological developments. The emerging threats such as AI-generated deepfakes, image morphing, and hyper-realistic synthetic content require proactive laws and guidelines to prevent exploitation and enable effective prosecution.
8. The digital platforms and intermediaries should be held accountable through enforceable regulations. The periodic audits, mandatory content moderation protocols, and collaboration with law enforcement can help mitigate the risks posed by advanced technologies and ensure safer online spaces.

## IX. CONCLUSION

The internet has evolved into more than just a tool for communication, it has become a mirror reflecting how we think, feel, and act. This "internet-guided behaviour" has significantly influenced the way individuals present their lives online, often blurring the boundaries between personal privacy and public exposure. While the digital space enables expression and connectivity, it also opens the door to various forms of abuse, especially targeting women and children. Incidents of cyberbullying, online stalking, image morphing, and the circulation of Child Sexual Exploitation and Abuse Material (CSEAM)) reveal the disturbing reality of exploitation that continues to thrive behind the screens. These digital crimes call for urgent, systemic interventions that go beyond individual action and require robust legal and institutional safeguards.

In recent years, judiciary has played a significant role in acknowledging and addressing online exploitation, particularly through landmark judgments that have pushed for stronger institutional safeguards. Alongside these efforts, legal frameworks and executive measures have been introduced to strengthen protections, including specialized reporting portals and cybercrime units. However, despite these developments, gaps remain in implementation, inter-agency coordination, rapid technological developments such as AI-generated deepfakes and the ability to respond effectively to complaints, especially in sensitive cases involving minors and vulnerable users.

Despite the challenges, the growing attention to digital safety from various institutions reflects meaningful progress. With continued efforts, greater accountability, and a shared commitment to creating safer online environments, there is hope that digital spaces can become more secure, inclusive, and respectful for all users, especially for those most at risk.

## X. REFERENCE

**A. Treaties and International Instruments:**

1. Convention on the Elimination of All Forms of Discrimination Against Women, 18 December 1979, 1249, UNTS 13.
2. Declaration on the Elimination of Violence Against Women, GA Res 48/104, UN GAOR, 48th Sess, Supp No 49, UN Doc A/RES/48/104 (20 December 1993).
3. Beijing Declaration and Platform for Action, UN Fourth World Conference on Women, UN Doc A/CONF.177/20 (15 September 1995).
4. Council of Europe, Budapest Convention on Cybercrime, ETS No 185 (23 November 2001).

**B. Indian Legislation and Rules:**

1. The Information Technology Act, 2000.
2. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), 2011.
3. The Protection of Children from Sexual Offences (POCSO) Act, 2012.
4. The Indian Penal Code, 1860.
5. The Protection of Women from Sexual Harassment at Workplace Act, 2013.
6. The Digital Personal Data Protection Act, 2023.
7. The Bharatiya Nyaya Sanhita, 2023.
8. The Bharatiya Sakshya Adhiniyam, 2023.

**C. Books, Reports, and Journal Articles:**

1. Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' (2005) 23 *John Marshall Journal of Computer and Information Law* 659.
2. United States Department of Justice, Criminal Division, *Report on Online Child Exploitation Trends* (2023).

3. United Nations Office on Drugs and Crime, *Cybercrime and Victimisation: Challenges and Responses* (UNODC 2019).
4. National Crime Records Bureau, *Crime in India 2023: Statistics Volume II* (Ministry of Home Affairs, Government of India, 2025) https://www.ncrb.gov.in/uploads/files/2CrimeinIndia 2023PartII2.pdf accessed 26 December 2025.
5. ECPAT International and ECPAT Luxembourg, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (2016) 20.
6. Livingstone S, Carr J and Byrne J, *One in Three: Internet Governance and Children's Rights* (UNICEF Office of Research-Innocenti, 2016) https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html accessed 28 December 2025.
7. Kemp S, *Digital 2023: India* (Datareportal, January 2023) https://datareportal.com/reports/digital-2023-india accessed 20 December 2025.
8. Pathak A and Tripathi P, 'Digital Victimization of Women in Cyberspace: An Analysis of Effectiveness of Indian Cyber Laws' (2023).
9. *Online Safety for Children: Protecting the Next Generation from Harm* (NITI Aayog, Government of India, 2023) http://niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-from-harm.pdf accessed 26 December 2025.
10. Tripathi S and Singh N, 'Digital Child Abuse, the Danger of AI-Based Exploitation' *The Hindu* (3 April 2025).

**D. Press Releases and Online Sources:**

1. Press Information Bureau, 'Cyber Crime Prevention against Women and Children Scheme, PIB (25 January 2020)' https://pib.gov.in/PressReleseDetailm.aspx?PRID=1600505 accessed 28 December 2025.

2. Central Bureau of Investigation, 'CBI Today Conducts National Wide Searches in Meticulous Operation in Megh Chakra at Around 59 Locations in 21 States/UT etc. in Two Cases Related to Download/Circulation of CSAM (24 September 2022)' https://cbi.gov.in/press-detail/NTI2Ng== accessed 28 December 2025.
3. ET Now Digital, 'COVID-19 Lockdown Sees a Surge in Online Child Sexual Abuse Cases', *Times Now* (22 April 2021) https://www.timesnownews.com/mirror-now/in-focus/article/covid-19-lockdown-sees-a-surge-in-online-child-sexual-abuse-cases/744764 accessed 20 December 2025.