
ONLINE CHILD SEXUAL ABUSE & THE ROLE OF INTERMEDIARIES

Vatika Chaudhary, Advocate, New Delhi

ABSTRACT

As the world seemingly moves forward, it makes us question the growth we have made as a society and as a legal system, given- the direction we are headed towards as an entire species when it comes to ever increasing abuse rates against the supposedly weaker parts of the society. Children and women are most vulnerable to all kinds of sexual abuse as they are perceived as easy victims. There have been increasing instances of children being subjected to sexual abuse even in the vicinity of family environment and the virtual space is definitely not the safest place to be for a child without adult supervision. The offences against children which include online harassment have become more prevalent with the advent of artificial intelligence and longer presence on social media. This paper focuses on the existing legal framework in the country with respect to the offences of online abuse committed against children. The research talks about the developments in laws and expansion in their interpretations to align them with the emerging technologies, their changed usages and misuses to commit offences which were implausible some time ago. It also highlights the shortcomings in the system that proves to work against an effective and timely action oriented approach and suggests the possible solutions including effective prevention strategies. The information we make available online, especially in case of kids and teenagers with their whole life ahead, needs to be maintained and put out very carefully as we are not aware of the places it can end up in. The sensitivity of the terms casually used in context of material containing sexual content involving children can be a matter of concern as it can diminish its nature to mere erotica available online and can devalue it as a criminal offence. The paper centers upon the fact that while keeping in mind the sensitivity of the topic, appropriate preventive techniques and remedial actions including deterrent penal measures, are very crucial without leaving room for loopholes.

Keywords: Sexual Abuse, CSEAM (Child Sexual Exploitation and Abuse Material), Intermediaries.

ONLINE CHILD SEXUAL ABUSE & THE ROLE OF INTERMEDIARIES

During the nascent stages of life, many children face horrors they never thought possible. Sexual abuse is one of the most abhorrent forms of these horrors that hover around the victims for the rest of their lives on both mental and psychological planes. When a child gets sexually abused, their body remembers it for far longer than a non-victim can comprehend. Even when they don't know what has happened to them, the feeling that something wrong took place, "they" being at the centre of it, always stays. And when they enter the later stages of life and get a grasp on what had exactly happened, it gives birth to a lifelong trauma with a feeling of betrayal that they had to go through it when they thought they were in the care of 'adults' of the society, their family, their peers and other responsible elders they were taught to trust. Sometimes it's not even the adults but their fellows and it's disheartening to know that this is not very uncommon today. Bringing a child in this world and raising them with utmost care, caution and dignity is much more difficult now than it has ever been.

If we think we can protect our children by keeping them inside the four walls of a house, we are mistaken as life is now happening online for most people around the globe. No generation is left untouched by the shackles of constant social media presence and detachment from the real world. Children are quick to pick up and good at navigating through technology than most adults. Internet and social media platforms can be a brilliant space to learn and grow, if we tune in to the right side of it. It can also be one of the most destructive and dangerous commitment we can get ourselves into, if we end up on the wrong foot. What is technically unreal or simply virtual, can get a life of its own in our heads and has a tendency to largely affect us in an impenetrable way, having real life consequences. Last few years have seen a huge rise in the cases of impact of online presence on our lives especially children or students having to take classes online and also turning to the internet for keeping themselves entertained throughout the day when lockdowns happened worldwide. The Covid-19 years have instilled in us an obsession and dependence on the virtual world, which is only growing by the day as we juggle between work and life and still try to find time to know everything that is happening online, irrespective of its relevance in our lives.

The most concerning part about virtual presence is the exploitation of data, information and the abuse that takes place on a daily basis with the most vulnerable users including children, women and people with limited understanding of the internet and associated risks. Here, we

are specifically focused on the sexual abuse that is enabled by the unsupervised use of internet and social media platforms by children. The digital realm facilitates the commission of sexual offenses against children through direct communication, the propagation of child sexual abuse imagery, and the coercive inducement of minors to produce and disseminate sexually explicit content, including through live streaming. Internet has proven to be a game changer in most of our lives, but for some, it has been/could prove to be the darkest place to be. The associated risks have taken a life of their own especially during the past 5 years where the internet has taken a soar like never before and we are basically living through it.

Types of online sexual abuse against children

It becoming a norm to hand out smart phones to children at an early age, the room for vulnerability expanded. Children are spending more time online than in any other real life pursuit. It is leading to damage in multiple areas of their lives and making them screen dependant from an early stage, leaving little to no room for cognitive development free from virtual stimulation. Another and the more concerning part is their exposure to the wrong end of internet and the lifelong resultant impact on their lives. Internet can be a terrifying place if we don't use it mindfully. Children, being unaware of the damage that people are capable of inflicting, are more prone to these horrors than others. Using the advantage of connectivity that internet allows, the abusers get an easy access to their victims especially when there is an unsupervised use by children. When shared or family devices are used without supervision, individuals become vulnerable to harmful content like pornography, violent material, and algorithmic manipulation. Amongst the many type of sexual abuse and advances made online, there are few more prominent ones that are going to be discussed here.

- **Child grooming**

Child grooming involves an adult befriending a child online with the intent of sexual abuse, often by exploiting the child's interests to build trust. Perpetrators, typically male, assess detection risks and isolate the child by emphasizing secrecy. The ultimate goal is sexual exploitation, either through manipulating the child into sending explicit content or arranging in-person meetings for abuse¹. Predominantly carried out by men, groomers use a child's online

¹ Ribhu Bhuwan, "Safe systems online: Child protection in a digital world", Deccan Herald : <https://www.deccanherald.com/technology/safe-systems-online-child-protection-in-a-digital-world-3534818>

information to feign shared interests and establish trust. Before escalating to sexual exploitation, they gauge the risk of being caught, often inquiring about parental monitoring of the child's online activities. It is easy for a child to access social media account by setting at naught the age restrictions by lying about their actual age². Platforms like facebook, instagram and public chat groups are used by the perpetrators to lure kids into being friends with them and access their personal information in order to reach them with an objective of sexual gratification and abuse.

Law in India - The POCSO Act, 2012, in Section 11(vi), directly addresses cyber grooming, defining it as sexual harassment against a child with sexual intent for pornography or gratification. It states that: "A person is said to commit sexual harassment upon a child when such person with sexual intent entices a child for pornographic purposes or gives gratification"³. The maximum penalty for this offense is three years' imprisonment and a fine.

Section 67B of India's IT Act, 2000, explicitly prohibits child pornography and related grooming activities. While "cyber grooming" isn't a direct term used here in the Act, it is covered by punishing those who "cultivate, entice, or induce children into online relationships for sexually explicit acts"⁴. The punishment provided for the said offence under IT Act is more than that provided under POCSO and extends to 5 years of imprisonment on first conviction along with a fine of upto 10 lakh rupees which points out the inconsistency between both laws for the same offence.

- **Cyber stalking/cyber harassment**

Cyber stalking is a contemporary computer crime involving the persistent online tracking and surveillance of individuals, which invades their privacy⁵. This form of harassment severely impacts victims, instilling fear and feelings of being threatened. Perpetrators, typically men targeting women or adults targeting children, conduct these actions remotely using digital tools, feeling secure from physical retaliation due to the perceived anonymity of the internet⁶.

² Devika Agarwal, "Child grooming: India must take measures to protect children from online sexual abuse", Firstpost, <https://www.firstpost.com/india/child-grooming-india-must-take-measures-to-protect-children-from-online-sexual-abuse-3438528.html>

³ Protection of Children from Sexual Offences Act, 2012, Section 11(vi).

⁴ Infra note 6.

⁵ Dr. Sapna Sukrut Deo, "Cyber stalking and online harassment: A new challenge for law enforcement", Bharati Law Review, July-Sept., 2013.

⁶ Daniel Manoj et al., "Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation", Science Direct.

Continuous trailing and tracking of social media accounts and emails and sliding into personal chats which involves various forms of threats on non-engagement of the victim, is another part of it and it becomes more dangerous when a child is at the receiving end because they are unaware of the methods to opt for safety. Impersonation is a tactic used by offenders who create deceptive accounts with similar names and stolen images to trick a victim's contacts into unknowingly providing access to the victim's real online profiles.

Law in India – In the Information Technology Act, 2000, cyber stalking and cyber harassment was punishable but this provision was struck down by the Supreme Court after the ambiguous language and terms used in the provision posed risk of misuse⁷. Sections 509 and 354D of Indian Penal Code (now Sections 349 and 77 respectively), provide punishments for the offences of criminal intimidation using anonymous communication and stalking respectively. Section 11(iv) of the POCSO Act criminalizes sexual harassment against children, implicitly covering stalking. This occurs when someone, with sexual intent, repeatedly follows, watches, or contacts a child, whether in person or electronically.

- **Child pornography**

Child pornography is defined as any representation of a child in explicit sexual acts or of their sexual parts for sexual purposes, including the creation of such content. This material circulates widely online via various platforms and apps. A growing concern is the live streaming of child sexual abuse, where abuse is broadcast in real-time, often with viewer participation, and sometimes facilitated by digital payments. The internet's accessibility has led to a rise in child pornography, consequently increasing other heinous crimes like sex tourism and direct child sexual abuse. Even the people who are buying or paying for these videos are actually paying for the child to get raped and hence are equal perpetrators to the actual offenders. The long term availability of such material on the internet can ruin a person throughout their lives, forcing them to re-live their trauma again and again and a constant fear of losing their position in society.

- **CSEAM (Child Sexual Exploitation and Abuse Material)**

Across various parts of the world, the term 'child pornography' is being replaced with 'Child

⁷ Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73

Sexual Exploitation Material’ (CSEM) or ‘Child Sexual Exploitation and Abuse Material’ (CSEAM). The purpose is to avoid the use of term pornography alongside the word child because it depicts or carries in itself a sense of consent in the making and emitting of such content. It is necessary to distinguish the sexual material recorded and available online where consent was involved from the acts which are exploitative, forceful and an offence by their very nature and emanated without consent of a person. It is unfair and ignorant even for the law to use the word ‘pornography’ for offences of sexual exploitation committed against a child and circulated for the world to find, leaving behind a lifelong trauma for the victim.

The longer an image or CSEAM stays online, the more difficult it is to combat the distribution of it. The possibilities of easy and unhindered access to CSEAM have been increased multifold with the growth and development of internet. The availability of such material is untraceable a lot of times because of the use of dark web to access such prohibited and punishable content. The dark web is that section of the internet that can only be reached using special software, providing anonymity to both its users and the people running websites on it⁸. Some part of this web allows the users to upload and access prohibited content while being anonymous and untraceable, which cannot be otherwise legally done. A large part of dark web is devoted to illegal activities, which makes this place prone to availability of content like child sexual abuse.

Just Rights for Children Alliance vs. Harish & others⁹

A landmark judgment has been passed by the Supreme Court recently, concerning the issue of storing, preserving and watching of child pornographic material. This judgment points out the errors in the High Court's ruling regarding the scope of criminal liability under Section 15(1) of the POCSO Act and Section 67B of the IT Act, 2000. Authored by former Hon’ble CJI D.Y. Chandrachud and Hon’ble Justice J.B. Pardiwala, this judgment emphasizes on the need for sensitization of legal terminology including the use of the term CSEAM (Child Sexual Exploitation and Abuse Material) instead of ‘child pornography’ which trivializes the impact and the offense itself.

In this case, the respondent was in the habit of watching and downloading pornographic

⁸ Kurt Baker, “The dark web explained”, <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/darkweb/#:~:text=The%20dark%20web%20is%20a%20common%20gathering%20place%20for%20hackers,ransomware%2C%20or%20other%20malicious%20files.>

⁹ Just Rights for Children Alliance vs. Harish & others (2024) INSC 716

material on his device. For an offense under Section 14 of the POCSO Act, 2012, as well as under Section 67B of the IT Act, transmission or propagation of the possessed material is an essential element and the complaint is not maintainable without proof of transmission and propagation, which is absent here. Likewise, criminality under Section 292 of the IPC, 1860, requires the publication of obscene material, which is not applicable to the present facts. Therefore, before the High Court of Madras, the criminal proceedings were terminated after quashing of the charge sheet.

In the petition before the Supreme Court, it was contended that the provisions were overlooked by the High Court while dealing with the case and that watching and storing of child pornographic material is punishable under Section 15 of POCSO Act, 2012. The Supreme Court made a categorical interpretation of Section 15 in order to avoid any ambiguity. The court observed that the marginal note has to be considered with the Section and hence downloading and storing child pornographic material and failing to delete it, is an offence under this provision, whether with an intention to propagate and transmit it or not. The court reiterated that it is no longer important to look at the intent as long as a sexual offence is being committed against a child.

The Hon'ble Court also laid down guidelines to be followed in similar matters including the use of CSEAM (Child Sexual Exploitation and Abuse Material) instead of 'Child Pornography' by every court in such matters. Implementation of sex education programs and generating awareness, which has a crucial role of school authorities, is also suggested by the court. The court also emphasized the need for rehabilitation programs for offenders and support services for the victims of such offences along with the constitution of an Expert Committee by the Government of India for providing a mechanism for sex education.

Liability of Intermediaries

Under Information Technology Act, 2000, 'Intermediary' has been defined as 'any person, who on behalf of another person receives, stores, transmits that record or provides any service with respect to electronic record'¹⁰. It is the intermediaries that provide a platform for making any information or data content available online for the users to access, download, store or modify. It should be the responsibility and duty of intermediaries to prevent the use of their platform

¹⁰ Information Technology Act, 2000, Section 2(1)(w)

for unlawful activities and to remove such content with immediate effect in order to prevent its propagation. The Hon'ble Court held that Intermediaries are accountable and duty bound to report such matters to the police.¹¹

There are many gaps in the Indian legal system and the existing strategies used to combat online child sexual abuse. The lack of detailed rules regarding the prior filtering and identification of the content made available online is one of the biggest problems that assist the spreading of such content without a timely detection and removal. The 'Safe Harbor Immunity'¹² provided to the intermediaries is highly misused and leads to evading of liability in related matters. It must be made mandatory for the intermediaries to keep a complete and systematic track of the activities on its platform which can be utilized for both prevention and at the stage of investigation in an offence committed using their platform.¹³ The IT Act, 2000 does not make it mandatory to report child sexual abuse. The intermediaries including the Internet Service Providers, social media platforms, web browsers, must be made responsible for reporting of instances of online abuse involving a child. Under the POCSO Act, 2012, Sections 19 and 20 places a responsibility of reporting such matters to the appropriate authorities but only limited to offences under POCSO Act and is not extended to offences under IT Act.

The concept of age verification when visiting and using a website or an online platform is a mere formality which is heavily dependent on self declaration without the supervision of adult members of the family. Tech companies must be held responsible for becoming an enabler of sexual abuse of children irrespective of the intent. The Hon'ble Supreme Court also reiterated that it is no longer important to look at the intent as long as a sexual offence is being committed against a child.

The Digital Personal Data Protection Act, 2023

The DPDP Act of 2023 mandates certain responsibilities for organizations handling children's personal data. The DPDP Act, 2023 also prohibits the data fiduciaries¹⁴ from tracking and

¹¹ Supra note 9

¹² Information Technology Act, 2000, Section 79 - provides immunity to an internet intermediary from liability under all laws, provided the intermediary has not conspired, abetted, aided, or induced the commission of an unlawful act or upon receiving actual knowledge through any notification about a computer resource in the control of the intermediary being used for an unlawful act, and fails to expeditiously remove or disable access to that material.

¹³ Supra note 6

¹⁴ Digital Personal Data Protection Act, 2023, Section 2(i) - "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

monitoring the behavioral use of internet by children except for certain purposes like health, education and learning etc. This Act emphasizes on the need for parental consent before using various services on the internet. The DPDP Rules, 2025 have been proposed with emphasis on protecting minors from privacy violations in the cyberspace and protection from heinous crimes that can be committed using internet as a medium. It explains the procedures that need to be followed in order to get verified consent from parents in case of social media use by minors¹⁵. Countries like Australia has gone a step further and banned the use of social media platforms by children below the age of 16 years¹⁶. A hefty fine is planned to be imposed by the Australian law on the companies which do not follow the guidelines to verify the age of the users and for allowing kids to use social media platforms. It is a strict but welcome step considering the ill impacts of social media usage among the youth, specifically the children unaware about the terrors of social media and their long term impacts.

Offences, using the internet, can not only be committed against children but through children as well because it is the easiest way to lure a child into a trap while maintaining anonymity with the end objective of committing crimes via then and remaining untraceable. Parental consent and regulated monitoring is a welcome step but it does come with certain loopholes and the implementation becomes difficult because a child can just enter false information and use such platforms and can also access the prohibited parts of the internet through their parents account as many people use shared devices. Also, there is information which is publically available already which involves minors and the details about them and are already prone to access by anyone. The digital illiteracy amongst parents make them dependant on their children to teach them and navigate through the use of internet and social media platforms and in such cases, the responsibility does not lie on the parents because they are themselves reliant on their children for even basic internet uses¹⁷.

¹⁵ Aishwarya Paliwal & Himanshu Mishra, "Parental consent must for children's accounts: Centre in draft social media rules", India Today, <https://www.indiatoday.in/india/story/centre-in-draft-rules-for-data-protection-parental-consent-must-for-children-to-open-social-media-account-2659474-2025-01-03>

¹⁶ Chris Stokel-Walker, "Social media bans for teens: Australia has passed one, should other countries follow suit?", The Guardian, <https://www.theguardian.com/media/2025/feb/22/social-media-bans-for-teens-australia-has-passed-one-should-other-countries-follow-suit>

¹⁷ Shreya Shekhar, "Parental Consent as the New Log-in Password for Children: Analysing the Draft Digital Personal Data Protection Rules, 2025", Law Review, NMIMS, <https://lawreview.nmims.edu/2025/04/05/parental-consent-as-the-new-log-in-password-for-children-analysing-the-draft-digital-personal-data-protection-rules-2025/>

CONCLUSION

A survey report suggested that in the age range between 14 and 16 years, more than 57% children use smart phones for the purposes of education whereas the percentage for usage by children for the purpose of social media is a whopping 76%¹⁸. India is amongst the top most countries when it comes to social media usage and a large part of it includes children and teenagers who have early access to such platforms before they can even fully comprehend the risks and repercussions involved. As has been observed, our country has a strong legal framework which allows it to penalize the offenders in cases of sexual abuse of children. The problem lies in the discrepancies between laws with respect to the same offences, which leads to confusion and interpretation issues. The POCSO Act, 2012 and the IT Act, 2000 must be in harmony when it comes to offences of online sexual abuse against children. As compared to our more technologically advanced western counterparts, India is behind in preventive strategies and stricter rules for pre-filtering of sexual abuse material that is posted or made available online. This needs to be regulated at the base level, at the level of its introduction online so that its further distribution can be stopped. The role of Internet Service Providers is very crucial at this stage. They must be strictly held responsible for regulation on their part including the blocking of websites and groups which contain content of child sexual abuse, prohibiting the uploading of such content on their platform, terminating and taking action against such accounts dealing in such abusive materials and so on.

With the advent of newer technology and developments in Artificial Intelligence every passing day, it is incumbent upon us to take the responsibility of updating and formulating stricter and consistent laws and regulations to protect the children from the horrors of sexual abuse capitalizing the universally and easily accessible mode of internet. To protect the children is to protect and to provide a healthy environment for these children to grow into adults who are not burdened by the lifelong trauma of carrying such terrors with them throughout their lives, to give them opportunities to live a good life and basically to protect their basic human rights from being brutally violated in the incipient stages of their lives.

¹⁸ The annual Status of Education Report (ASER), 2024.

References

“76% kids aged 14-15 using smartphones for social media, usage more among boys than girls: Report”, Hindustan Times, <https://www.hindustantimes.com/india-news/smartphone-usage-in-india-among-14-15-years-kids-report-on-digital-device-among-boys-and-girls-social-media-101738075735047.html>

“Online child sexual exploitation and abuse”, Module 12, Interpersonal Cybercrime, United Nations Office on Drugs and Crime, <https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html>

Aditi Verma Thakur Anju Srinivasan, “Safe Harbour Immunity for internet intermediaries and ip violations: where we stand today and the way forward?”, Volume II, Journal of Intellectual Property Studies, <https://induslaw.com/app/webroot/publications/pdf/alerts-2019/safe-harbour-immunity-for-internet-intermediaries-and-ip-violations-where-we-stand-today-and-the-way-forward-converted.pdf>

Aishwarya Paliwal & Himanshu Mishra, “Parental consent must for children's accounts: Centre in draft social media rules”, India Today, <https://www.indiatoday.in/india/story/centre-in-draft-rules-for-data-protection-parental-consent-must-for-children-to-open-social-media-account-2659474-2025-01-03>

Aman Singh Bakshi, “Bois Locker Room”: The role of Intermediaries in regulation of content”, Bar & Bench, <https://www.barandbench.com/columns/bois-locker-room-the-role-of-intermediaries-in-regulation-of-content>

Chris Stokel-Walker, “Social media bans for teens: Australia has passed one, should other countries follow suit?”, The Guardian, <https://www.theguardian.com/media/2025/feb/22/social-media-bans-for-teens-australia-has-passed-one-should-other-countries-follow-suit>

Chris Stokel-Walker, “Social media bans for teens: Australia has passed one, should other countries follow suit?”

Daniel Manoj et al., “Behind the screens: Understanding the gaps in India’s fight against online

child sexual abuse and exploitation”, Science Direct.

Devika Agarwal, “Child grooming: India must take measures to protect children from online sexual abuse”, Firstpost, <https://www.firstpost.com/india/child-grooming-india-must-take-measures-to-protect-children-from-online-sexual-abuse-3438528.html>

Digital Personal Data Protection Act, 2023, <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>

Dr. Sapna Sukrut Deo, “Cyber stalking and online harassment: A new challenge for law enforcement”, Bharati Law Review, July-Sept., 2013.

Information Technology Act, 2000, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Just Rights for Children Alliance vs. Harish & others (2024) INSC 716, <https://www.dhyeyalaw.in/just-rights-for-children-alliance-v-s-harish>

Kurt Baker, “The dark web explained”, <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/darkweb/#:~:text=The%20dark%20web%20is%20a%20common%20gathering%20place%20for%20hackers,ransomware%2C%20or%20other%20malicious%20files.>

Palak Nigam, “Child pornography in India: A study from socio-legal perspective”, Manupatra, <https://articles.manupatra.com/article-details/CHILD-PORNOGRAPHY-IN-INDIA-A-STUDY-FROM-SOCIO-LEGAL-PERSPECTIVES>

Protection of Children from Sexual Offences Act, 2012, <https://www.indiacode.nic.in/bitstream/123456789/2079/1/AA2012-32.pdf>

Ribhu Bhuwan, “Safe systems online: Child protection in a digital world”, Deccan Herald : <https://www.deccanherald.com/technology/safe-systems-online-child-protection-in-a-digital-world-3534818>

Shreya Shekhar, “Parental Consent as the New Log-in Password for Children: Analysing the Draft Digital Personal Data Protection Rules, 2025”, Law Review, NMIMS,

<https://lawreview.nmims.edu/2025/04/05/parental-consent-as-the-new-log-in-password-for-children-analysing-the-draft-digital-personal-data-protection-rules-2025/>

Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73, <https://www.dhyeyalaw.in/shreya-singhal-v-union-of-india>

The annual Status of Education Report (ASER), 2024, <https://asercentre.org/aser-2024/>