VULNERABLE ONLINE

A STUDY ON CYBERCRIMES AGAINST CHILDREN IN INDIA

INDIA CHILD PROTECTION

Cover Image: AI Generated

VULNERABLE ONLINE

A STUDY ON CYBERCRIMES AGAINST CHILDREN IN INDIA

Introduction

A study published in April 2020 by the India Child Protection showed that the consumption of child pornography increased by 95 percent since the nationwide lockdown in March. This spike in consumption is indicative of the fact that paedophiles have migrated online making the internet an extremely unsafe place for children. The report shows that there is an increase in demand for searches like “child porn”, “sexy child” and “teen sex videos”. Moreover, there is also an increase in demand for violent content involving children. This is a huge concern for children who have also begun using the internet much more now than ever before due to online classes during the pandemic-induced lockdowns. Often, children are using internet without adult supervision. This makes them even more vulnerable to such perpetrators and crimes like cyber-trafficking, grooming, sextortion and live streaming of child sexual abuse. More and more wide and spread-out cybercrimes are emerging as offenders are finding new and diverse methods to exploit children's unaware and neglectful attitude in cyberspace. In other words, “new technology often coincides with new ways of misuse or abuse of that technology” (Fourie, 2020, p.231).

Legal Sevice India (Narnolia, n.d.) notes that India is the second largest online market with over 560 million users of internet, the largest market being China. It is estimated that there will be over 650 million users from India by 2023. It is then imperative to understand the world of internet and cyberspace in general. On the one hand, digital technology and its fast growing progress has proven to be beneficial for people and especially children, but on the other hand, there is also the dark truth of it proving to be detrimental and exploitative for children.

The increasing prevalence of online child sexual abuse material led to significant legal scrutiny, particularly following the case of S. Harish in Tamil Nadu. In January 2020, following a Cyber Tipline Report from the NCRB, Tamil Nadu police registered an FIR under the POCSO Act after it was discovered that Harish had been an 'active consumer' of child pornography. Upon further investigation, it was found that the videos Harish had contained involved children who had been missing and were exploited. Despite this, the Madras High Court, in January 2024, ruled that 'mere possession or storage' of child, pornography was not an offence under the POCSO Act, and further declared that Harish was not guilty under Section 67B of the IT Act, which only makes it illegal to "transmit, publish, or create" child pornography—not to "watch" or "download" it, sparking widespread concern. On 22 February 2024, the NGO 'Just Rights for Children Alliance' (JRCA) appealed against this ruling in the Supreme Court arguing that the ruling would give the 'general public' the impression that 'downloading and possessing child pornography is not an offence, potentially increasing the demand for child pornography and encourage people to involve innocent children in pornography'. On 23 September 2024, the Supreme Court overruled the High Court, holding that mere viewing, possession and storage of material depicting minors engaged in sexual activity constitutes an offence under the POCSO Act

and Section 67B of the IT Act. It was also observed that in a case of 'child pornography' while the victimisation of the minor starts with the sexual act, it continues and deepens with the recording of the act, the perpetuation of photos and videos, and creates a ripple of trauma for the child. And, hence it was proposed that 'Child Sexual Exploitation and Abuse material' abbreviated as 'CSEAM' was a more appropriate terminology for the heinous act, instead of 'child pornography'.

"Cybercrime refers to any crime performed using a computer or an electronic device, mainly through the Internet" (Deora and Chudasama, 2021, p.1). Since most internet use is on mobile phones and given the fact that mobile phones have become such important parts of our lives, susceptibility to fall for cybercrimes too has become tied to our lives. While cybercrimes have been a growing problem since the 1990s itself, cybercrimes against children especially have increased exponentially since COVID-19 and the subsequent lockdowns globally. The National Crime Record Bureau recorded a 25 percent increase in cybercrimes against children in 2021 (1376 cases in 2021 from 1102 cases in 2020) and a further 32 percent increase in 2022 (1823 cases). It is then an important theme to explore and analyse for a better understanding and resolution of the issue.

Key Highlights of the Judgement

- **Section 15(1) of the POCSO Act states that 'any person, who stores or possesses child pornography' and 'fails to delete or destroy or report' it can be punished with a fine of up to five thousand rupees, and on subsequent offence, up to ten thousand rupees. Section 15(2) states that if the possession and storage are with intent of "transmitting or propagating or displaying or distributing," that can lead to a higher punishment of up to three years imprisonment. Various High Courts have held that the intent to distribute or commercially use such content was crucial for a Section 15 offence to be made out. The Supreme Court clarified that each of the subsections of Section 15 carve out independent offences.**
- **Section 67B of the IT Act penalises the 'publishing' and 'transmitting' of child pornography. The Court ruled that Section 67B not only punishes 'electronic dissemination' of child pornographic material but also the 'creation, possession, propagation and consumption of such material'.**
- **Even accessing CSEAM online, regardless of storing or distributing the material, amounts to 'constructive possession' of such content and is punishable under Section 15 of the POCSO Act. Constructive possession occurs when a person has control or access to such material, even if it's stored digitally or on a device not directly in their hands.**
- **Section 30 of the POCSO Act states that for any POCSO offence, the Special Court 'shall' presume that the accused had a culpable mental state.**

Essentially, if certain "foundational facts" are established prima facie, the burden is on the accused to show that he was not guilty. For instance, the Court noted that for a Section 15(1) offence, the prosecution has to only show the foundational fact that the accused was in possession of child pornography and did nothing to get rid of it or report it.

- It was observed that in a case of 'child pornography' while the victimisation of the minor starts with the sexual act, it continues and deepens with the recording of the act, the perpetuation of photos and videos, and creates a ripple of trauma for the child. Furthermore, it was proposed that 'child sexual exploitation and abuse material' abbreviated as 'CSEAM' was a more appropriate terminology for the heinous act, instead of 'child pornography'.
- The Judgement urges Parliament to 'seriously consider' amending the POCSO to substitute 'child pornography' with 'CSEAM'. It urged the Union to consider bringing about the suggested amendment through an ordinance, to ensure swift action. It also issued notice to all courts to not use the term 'child pornography' in judicial orders and judgements.
- The Judgement reiterated that Sections 19 and 20 of the POCSO Act imposes an obligation on persons, and media, hotel staff, hospital staff, clubs and studios to mandatorily report or give information about any child pornographic material. Section 21 states that failing to do so would result in imprisonment of up to six months.
- It also noted that Rule 11 of the POCSO Rules obligated intermediaries to hand over necessary material including the source of the material to the Special Juvenile Police Unit or local police or cyber-crime portal.
- The Court also made a notable observation on Section 79 of the IT Act. Section 79, also known as the 'Safe Harbour' provision, protects intermediaries from liability for any third-party information, data or communication link available or hosted on the intermediary. The Court, however, clarified that the 'Safe Harbour' protection does not apply to child pornography.
- The Court directed the Ministry of Women and Child Development to implement comprehensive sex education programs to create awareness on legal and ethical ramifications of child pornography. It also directed that victims of child pornography be provided psychological counselling, therapeutic interventions, and educational support.
- The Court directed the Union to constitute an Expert Committee that would devise a comprehensive program for health, sex education and POCSO awareness among children.

Literature review

The 2020 Child Safety Online Index, a survey of 30 countries conducted during the pandemic's first year, ranks India ninth (with an 'average' rating) for having the "best online safety for children" but second in terms of the "extent of cyber-risks" faced by children. This seems to indicate that children in India face a high volume of risks online, but that the efficacy in dealing with these risks is "average" (Sarma, 2022).

Nearly 61 percent of the total cybercrime cases in 2021 were done with the motive of committing fraud. Sexual exploitation emerged as the second-most common motive for committing cybercrimes (Krishnakumar, MoneyControl, 2022). It amounted to 8.6 percent of the total cybercrimes committed. However, in the case of children especially, nearly 90 percent of the rise in cybercrimes in 2020 "involved the publication or transmission of child sexual abuse material" (Sarma, 2022). In 2021, 6598 total cases of publishing or transmitting obscene or sexual content were reported. Increasingly then, it is being seen that cybercrimes that are sexually exploitative in nature are on the rise and this is certainly a growing problem that needs to be dealt with immediately.

There are several risks involved in online sexual abuse and exploitation of children and equally difficult is the detection and investigation of these crimes. This section will first enlist the kinds of cybercrimes prevalent against children, then talk about the availability and consumption of online material involving sexual crimes against children. It then goes on to define the kinds of risks that children face, legislations to curb such crimes and finally, discuss the difficulties encountered in reporting and investigation.

Types of cybercrimes against children

Online child sexual abuse and exploitation: One of the most prominent and equally disturbing crimes against children is sexual abuse and exploitation. In the world of internet, the risks, effect and disappointment faced by children increases because of its permanence. Protection of Children from Sexual Offences Act, Section 13 defines the crime as use of "a child in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification, which includes representation of the sexual organs of a child usage of a child engaged in real or simulated sexual acts (with or without penetration) and the indecent or obscene representation of a child."

Grooming:

Grooming refers to "a method of building trust with a child and adults around the child in an effort to gain access to and time alone with her/him." (Gasser and Cortesi, 2017).

Cyberstalking:

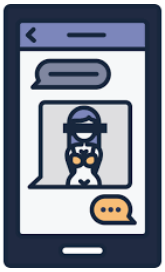
According to Section 354D of IPC, stalking refers to "following a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman" and cyberstalking refers to monitoring "the use of internet, e-mail or any other form of electronic communication" by a woman or a child. This is usually for the purpose of trapping, blackmailing or sexually exploiting them.

Cyber bullying:

The Indian Penal Code does not recognise bullying as a crime however, in NCRB, cyber bullying is clubbed with cyberstalking. Cyber bullying refers to a form of harassment using electronic means where a person forces or coerces someone in order to threaten, dominate or intimidate them.

Cyber blackmailing:

Cyber blackmailing or online sextortion occurs when someone threatens to distribute private and sensitive material using an electronic medium if he/ she doesn't provide images of a sexual nature, sexual favours, or money.



Sexting: Sexting refers to sending or receiving sexually explicit messages or images, mostly on mobile phones.

Online Trafficking: The practice of buying and selling children online mostly for sex and prostitution. Sometimes, websites also auction children through images procured while stalking them and tracking their movements.

Availability and consumption

As seen from the report by ICP (mentioned earlier), consumption of online CSEAM spiked manifolds during the COVID-induced lockdowns. In 2020, National Commission for Protection of Child Rights (NCPCR) issued notices to online platforms like Google, Twitter, WhatsApp and Apple India warning them of spikes in online CSEAM based on ICP's report (Pandit, TOI, 2020). The NCPCR then went on to hold an independent inquiry into the availability of online CSEAM. There have been various efforts to identify report and curb the spread of online CSEAM globally since US-based National Center for Missing and Exploited Children (NCMEC) started urging people to report any kind of child pornography encountered online. According to the NCMEC, about two million cases of child sexual abuse are being reported every year in India (Akhawat, DeccanHerald, 2022).

In India, the Central Bureau of Investigation (CBI) began an operation named Operation MeghChakra in September 2022. They conducted nationwide raids in 21 states and union territories and arrested close to 50 suspects along with confiscating their electronic devices. The operation is targeted at cloud storage facilities used by the criminals to circulate audio-visuals of illicit sexual activities with minors, which is why it is called MeghChakra (megh means cloud in Hindi). These searches were based on information provided by Interpol and upon preliminary inspection of the confiscated electronic devices, several CSEAM were found (Pandey and Singh, IndiaToday, 2022). Other such attempts have been Operation Blackface in Maharashtra, the investigating attempt of cyber department and state police started in 2019 that registered 213 FIRs and arrested 105 people across the state for "uploading child pornography and sexually explicit videos and photographs of minors on the internet" in a year and a half (Naidu, IndianExpress, 2021) and Operation Big Daddy in Kerala, another investigating attempt where a huge sex racket was revealed in Kerala in 2016 which involved women and children. In 2017, a group of ethical hackers in Kerala (who call themselves Mallu Cyber Soldiers) released the details of 59 Facebook groups or pages, which spread offensive materials on the internet, and deleted the entire content after receiving a lot of complaints from the users of the social media platform. The hackers claimed that more than 10,000 such pages are active in Malayalam language alone which are growing though they are repeatedly shut down (Raj, DeccanChronicle, 2017).

The availability and consumption of online CSEAM has been a growing problem in India. An online news article says that a report published in 2020 stated that India has seen a 95% increase in internet searches for CSEAM during the lockdown which is in tandem with the ICP report (HindustanTimes, 2021). Even the Delhi Commission for Women (DCW) chairperson stated that several tweets on Twitter openly post videos and photographs of sexual acts involving children. Some accounts engaging in these criminal acts seem to be running a racket wherein they seek money for providing pornographic and rape videos of children from other users of the social media platform (DNA, 2022). It is then clear that it is becoming much easier for paedophiles and other criminals to access online CSEAM which could easily lead to an increased number in cases of child sexual abuse and exploitation.

Risks

All crimes against children have severe effects on them, especially their mental health. It is important to note that cybercrimes have a unique feature of permanence attached to them that increases the severity of the crime. Knowing that a particular image or clip of an abusive and nonconsensual act exists and will always exist on the internet could affect a child's mental health acutely and often continues to hurt well in adulthood as well. According to a professor of child and youth development, "an exacerbating factor for many child victims is knowledge that a record exists of their abuse and the trauma, powerlessness, and shame they have experienced" (Harrison, 2006, p.370). In fact, research even shows that the psychological consequences of online child sexual abuse are similar to that of offline child sexual abuse. A cyber lawyer says that more often than not, minors fall victim to child pornography by people known to them, including relatives (Narayan, TOI, January 2022). This further harms the mental health of the child. "Child sexual abuse, both online and offline, in the absence of proper positive supportive experiences, leads to neuropsychological changes and dysfunctional coping mechanisms. The negative consequences include psychical, psychological and emotional impacts, such as depression, anxiety, PTSD (Post Traumatic Stress Disorder) and self-harm" (Caffo, 2021, p.2).

Studies on cybercrimes against children categorise these crimes into three types depending upon the kind of risk that a child is vulnerable to:

Content risks involve the receipt of unfavourable, violent, sexually explicit or hateful content. In this type of risk, the child is the recipient of negative content on the internet. According to EU Kids Online II Survey (2009-2010), "the biggest concern for children is around content risks, such as pornography and violent images (58%)" (Fourie, 2020, p.237).

Content risks are not limited to only sexually exploitative content but also include violence, religious discriminatory content, trolling and negative reactions or commentary from strangers online. "Other types of online material that children may find upsetting include violent videos and games, rude and insensitive comments, and scary pop-up advertisements, all of which can reduce children's enjoyment of the online experience" (Gasser and Cortesi, 2017, p.10).

Contact risks involve the risk of unwanted, vulgar or negative contact by adults. Contact may not necessarily mean physical contact but even virtual contact or contact on social media may prove to be dangerous to children, especially because they are "less careful whom they socialise with on the internet and would often share personal information, engage in undesirable exchanges" (Fourie, 2020, p.240). The child is a participant in such crimes.

Adult offenders often engage in cyberstalking, grooming, cyber solicitation with underage people in order to satiate their own desires and in exchange abusing and exploiting the children who fall for such advances. Internet provides anonymity and that is misused by offenders along with the child's ignorance.

Paedophilia has emerged as one of the most terrible online offences and is most prominent in many countries. "Paedophiles increasingly use technology to search the internet for potential child victims and are often part of organised crime" (Fourie, 2020).

Conduct risks involve children's own behavior and attitude online. While the discourse on cybercrimes against children focuses largely on the exposure of children to content and contact-related risks, there is also the risk of children themselves behaving in ways that could exploit them or other children. This is where the child is not merely a recipient or participant in the crime but is an actor.

Crimes such as cyberbullying or sexting are the most common in conduct risks. Revenge porn is another crime that children commit on one another. "Engaging in sexting can have severe negative consequences...including legal ramifications that children might not be aware of" (Gasser and Cortesi, 2017, p.11). A news report in 2012 noted that in a survey conducted by Microsoft (Global Youth Online Behaviour Survey), five in 10 children said that "they have experienced what adults might consider online bullying, while a similar number said they had done something their parents may consider online bullying."

Leveraging Technology and International Networks to Address Online Child Abuse in India

In India, there are majorly two ways of tackling the online CSEAM cases.

1. Direct reporting through the helpline number / cybercrime portal / police station, etc.
2. CyberTipline cases / data being received from international agencies.

When online child sexual abuse is reported through direct reporting, the local police immediately initiate an investigation and prosecution of offender. If necessary, information is shared with the cybercrime department to leverage their expertise in handling digital evidence and tracking online offenders. Intermediaries, such as internet service providers or social media platforms, are contacted to aid in the intervention process and sharing of evidence. Further efforts are made for helping the victim by extending various support for protection and rehabilitation.

Government of India has signed a Memorandum of Understanding (MoU) with the National Center for Missing and Exploited Children (NCMEC) on April 26, 2019. This MoU facilitates the receipt of Tipline reports on online child pornography and child sexual exploitation from NCMEC. This international agency collects all the CSEAM reports across various online / digital platforms which it further compiles and shares with the GoI as per the MoU. The flow of information is such that IP addresses found by NCMEC that are indulging in downloading and distributing online child pornography or CSEAM are shared.

Recently, Ministry of Home Affairs has created India Cyber Crime Coordination Center (I4C) and entered into agreement with NCMEC to share the CyberTipline data with I4C. The data, which was previously being shared with NCRB, is now being shared with I4C. The primary aim of this vertical is to tackle the increasing instances of online crimes against children and woman across India by enhancing prosecution and providing end-to-end assistance to the victims & their families.

FLOW OF INTEL RECEIVED FROM INTERNATIONAL AGENCY

NCMEC is a database repository, which collects all the CSEAM reports across various online / digital platforms.

↓

NCMEC compiles data, segregates and shares with India under the Memorandum of Understanding with I4C (earlier it was being shared with NCRB

↓

NCRB / I4C shares data with States/UTs through National Cybercrime Reporting Portal for further action

↓

State does further segregation and disseminates the data to district

↓

District further segregates and disseminates the data to local police station

↓

Investigation of case and conviction of offenders by the local police station

Challenges in the data received from NCMEC

India faces several significant challenges in effectively utilizing the cyber tipline data received from the National Center for Missing and Exploited Children (NCMEC).

- **Bulk Data and Filtration:** A significant challenge is the sheer volume of data received, which can be overwhelming. The bulk data dump requires immense time and effort for proper filtration and analysis. Law enforcement agencies need to sift through vast amounts of information to extract relevant and actionable intelligence, a process that is both time-consuming and resource-intensive. This leads to delay in investigation and prosecution of cases.
- **Data Duplication:** Data duplication is another challenge. When multiple reports pertain to the same or single CSEAM content / incident across various social media platforms, it can lead to redundancy in investigations. Law enforcement agencies may waste time reviewing the same information repeatedly, which delays the overall investigative process and hampers the efficient allocation of resources.
- **False Positives:** One of the major issues is the prevalence of false positives in the data provided. These inaccuracies can stem from errors in reporting or ambiguities in the photo / video, leading to investigations based on incorrect leads. This may include pixelated photo / video or even non-CSEAM content being classified as CSEAM.
- **Time-lapse:** Due to long time lapse, retrieving and collection of evidence from offender's device becomes a challenge as it can tampered / deleted / modified, etc which hampers the investigation of case.
- **Victim Identification:** Identifying victims from the CyberTipline data poses another critical challenge. Often, the data may not include sufficient details to directly identify or locate victims, such as names or specific locations. This lack of clear information complicates efforts to provide timely support and protection to those affected. Effective victim identification requires advanced forensic techniques and robust coordination among various agencies to piece together fragmented data and ensure the victims receive appropriate assistance.
- **Age verification:** There is no mechanism to verify the age of the person present in the media reported to NCMEC. At times, it becomes very difficult to identify whether the person is an adult or a child victim.
- **Encrypted data:** The CSEAM content being shared through WhatsApp messages / media files and other end-to-end encrypted platforms do not get detected or reported to NCMEC.

Legislations and other measures for curbing cybercrimes against children

India's commitment to child protection is evidenced by its early ratification of the UN Convention on the Rights of the Child (CRC) in 1990. This commitment was further strengthened in 2002 when India acceded to the Second Optional Protocol, which focuses on addressing online and offline offenses against children. This international framework has guided India in developing a robust legal framework to combat child sexual abuse and exploitation.

There are two main legislations in India that aim to curb cybercrimes against children – Sections 13, 14 and 15 of the Protection of Children against Sexual Offences Act, 2012 and Section 67B of the Information Technology Act, 2000. Apart from the legislations, the Ministry of Electronics & Information Technology started a programme called Information Security Education & Awareness through which it has been generating awareness on the risks and ethics of using the internet and the Ministry of Home Affairs is also implementing a scheme, Cyber Crime Prevention against Women and Children (CCPWC) under the Nirbhaya Fund through which it has provided grants to states and union territories encouraging them to set up cyber forensic cum training laboratories and to provide hands-on training to Law Enforcement Agencies (LEAs), investigators, prosecutors and judicial officers. The amount disbursed for CCPWC and for sub-projects under CCPWC is INR 142 crores out of the INR 224.76 crores appraised. This constitutes 3.2 percent of the total budget allocated in the Nirbhaya Fund till July 2022 (INR 4430.02 crores). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 further bolster digital platforms, particularly social media by ensuring that digital platforms identify and flag CSEAM and inform users attempting to access such content that is inappropriate. Additionally, sections of the Immoral Traffic Prevention Act offer a basis for addressing online child sexual abuse and exploitation. These include provisions related to the sale and circulation of obscene materials, sexual harassment, and criminal intimidation of children, online extortion, and child trafficking.

Table 1: Legislations against cybercrimes that are sexually exploitative in nature (for children)

Name of the Act and section	Description of crime	Extent of punishment
POCSO Act Section 14	The use of children for pornographic purposes.	Imprisonment for more than five years. If the same person is caught committing the crime again, then the punishment is imprisonment for more than seven years and a fine.
POCSO Act Section 15	The possession or storage of pornographic material involving a child or children.	If the offender does not delete or report the pornographic material, then it is assumed that they intend to transmit it. The punishment for this crime is a fine of more than INR 5000 and in the second instance, the fine is of more than INR 10,000.
IT Act Section 67B	Anyone who publishes or causes to publish sexually explicit material of children; creates, browses, downloads, exchanges or advertises such material; entices or cultivates children to have online relationships with other children thereby producing sexually explicit media; facilitates online abuse or exploitation of children; records sexual abuse of children electronically is liable to punishment according to this section of the Act.	Imprisonment for up to five years and a fine of up to ten lakh rupees. In the second instance, the imprisonment is for up to seven years and a fine of up to ten lakh rupees.
BNS Section 295	It prohibits the sale, distribution, or exhibition of obscene material to children under 18 years of age	Whoever sells, lets to hire, distributes, exhibits or circulates to any child any such obscene object as is referred to in section 294, or offers or attempts so to do, shall be punished on first conviction with imprisonment up to three years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, imprisonment up to seven years, and also with fine which may extend to five thousand rupees.

Indian Cyber Crime Coordination Centre

Indian Cyber Crime Coordination Centre (I4C) has been set up in 2018 by the Ministry of Home Affairs to combat cybercrimes more effectively. It has seven components viz. National Cybercrime Threat Analytics Unit, National Cybercrime Reporting Portal, Platform for Joint Cybercrime Investigation Team, National Cybercrime Forensic Laboratory Ecosystem, National Cybercrime Training Centre, Cybercrime Ecosystem Management Unit and National Cyber Crime Research and Innovation Centre.

Through I4C, the central government tries to spread awareness about cybercrimes, issues advisories and notices, does capacity building of authorities like police officers, judges and lawyers. Cyber Pravah, the quarterly newsletter of I4C covers the various initiatives taken by I4C and also states the cybercrime trends and patterns. This the Ministry of Home Affairs mentions on its website however, the journal is not available in public domain.

Other Initiatives

- **National Helpline Number:** Setting up and running of a national helpline number for reporting the incidents of OCSA.
- **Blocking of pornographic sites:** In August 2015, the GoI ordered ISPs to block access to over 857 pornographic websites due to concerns about child pornography. This decision was made under the Information Technology Act and Article 19(2) of the Indian Constitution. Although the complete ban was later lifted, the government continued to focus on blocking sites that hosted child pornography and illegal content.
- **Banning usage of sensitive key words / URLs:** Ministry of Home Affairs of India has prepared a list of certain keywords and URL sites, which are banned from usage and social media to enable a mechanism to show warning on searching the listed keywords and blocked URLs.
- **Australia–India Cyber and Critical Technology Partnership:** India and Australia have enhanced cooperation on cyber and technology issues through this partnership. The two countries engage in annual Cyber Policy Dialogues and working groups on cybersecurity and ICTs. Given their mutual commitment to child safety online, further collaboration could enhance efforts to build a safer cyberspace for children.
- **MOU with NCMEC:** India collaborates with various international entities to strengthen efforts against child pornography. The MoU with NCMEC exemplifies this collaboration, facilitating the exchange of information and technical assistance.
-

The problem of reporting and investigation

The quick and wide access to internet has made it extremely easy for predators to target unsuspecting children through social media and game forums while protecting their own identity with anonymity or fake ID. Moreover, "children all over the world are also starting to use the internet at an increasingly younger age...leaving many online policies lacking since they predominantly focus on children above 12 years" (Fourie, 2020, pp.230-231).

A study called Child Sexual Abuse: Awareness and Attitudes was published in 2020 by World Vision India that tried to understand the awareness on child sexual abuse and the willingness to report it. Out of 4500 parents/caregivers and 4500 children aged 12 to 18 years, 32.13 percent caregivers and 35 percent children were aware of the POCSO Act. Moreover, while 75 percent of caregivers felt confident that effective action would be taken in a child sexual abuse case, among children only 65 percent felt so. This marks a major barrier in reporting.

On the one hand, there is the problem of low reporting and on the other, there is the problem of investigating cases that are reported. Newspaper reports show that very few cases of cybercrimes are being converted into FIRs. This is one major reason for scammers and criminals not fearing the legislations that are in place to deal with cybercrimes. Current Home Minister of India also noted that the number of cybercrime cases that are not being reported could be in lakhs (Anand, CNBC, 2022). There is a lot to do in this realm then in order to improve the state of reporting cybercrimes, especially against children.

One problem of investigation is that of different jurisdictions not working together in the case of a cybercrime. As a paper written in 2017 notes, one major characteristic of online crimes is that "cross-national activity is much more common" in them. It is then very important for there to be "a degree of cooperation between states" which is often not very forthcoming (Chang and Grabosky, 2017). It can be inferred from this that even a degree of cooperation between different states within India is very significant and that too is not a very common occurrence.

Research objectives

In light of the increased use of digital technologies by children in India, especially after the outbreak of COVID, which makes them vulnerable to various types of crimes, this study has been undertaken to

1. identify the trends in cybercrimes against children in the last 5 years.
2. explore the types of cybercrimes committed against children with special reference to online sexual abuse and exploitation.
3. understand the disposal pattern of cybercrime cases.

Data source

The data for this study has been sourced from the Crimes in India reports of 2018 to 2022 published by the National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India.

Data analysis and discussion

Cybercrime trends in the last 5 years (2018-2022)

The number of cybercrime incidence reported in the country doubled in the last five years with a steadily rising trend. It increased from 27,248 in 2018 to 65,893 in 2022. The maximum increase in the number of cases was registered in 2019. As compared to 2018 the number of cases registered in 2019 increased by 63 percent.

On the other hand, in the case of cybercrimes against children, the reported incidences have increased 8 times in the last five years (232 in 2018 to 1823 in 2022). The maximum increase in these cases can be seen in 2020 where it increased by 261 percent. The substantial surge in cybercrime targeting children over the past three years (since the COVID-induced lockdown was imposed) is evident from the analysis. This is primarily because of children's growing usage of the internet, especially unsupervised use, brought on by online education.

Table 2: Total cases reported under cybercrimes and cybercrimes against children

Year	Total cases of cybercrime	Total cases of cybercrimes against children	Percentage distribution of cybercrimes against children to that of total cases
2018	27248	232	0.85%
2019	44546	305	0.68%
2020	50035	1102	2.20%
2021	52974	1376	2.59%
2022	65893	1823	2.76%

POCSO Act Sections 14 and 15 cases refer to online sexual offences against children. The trend of cybercrime cases under POCSO in the last five years (Figure 1) shows that registration of such cases increased by 37 percent (increased from 812 in 2018 to 1,114 in 2019). However, post 2019 the same started decreasing but saw an increase of 30 percent in 2022. As seen in the table above (Table 2) and will be seen later in cases of IT Act Section 67B (Figure 2) and cyberstalking and blackmailing cases (Figure 3), the cases of cybercrimes have increased in 2020 and 2021. This is in contrast to POCSO Act Sections 14 and 15 cases. The number of cases registered in 2020 and 2021 decreased by 48 percent and eight percent respectively as compared to the previous year. Even the percentage constitution of POCSO Sections 14 and 15 to total POCSO cases was highest in 2019 (2.35%) and lowest in 2021 (0.99%). The deliberate decision to not include POCSO charges in the FIRs may be to blame for the declining trend in POCSO case registration. It appears that in 2020 and 2021, cybercrime incidents were reported under Section 67B of the IT Act, cyber blackmailing/threatening/ harassment cases under Sections 384, 503 and 506 of IPC and cyberstalking/bullying cases under Section 354D of IPC.

Figure 1: Cases of POCSO Act and POCSO Act Sections 14 and 15

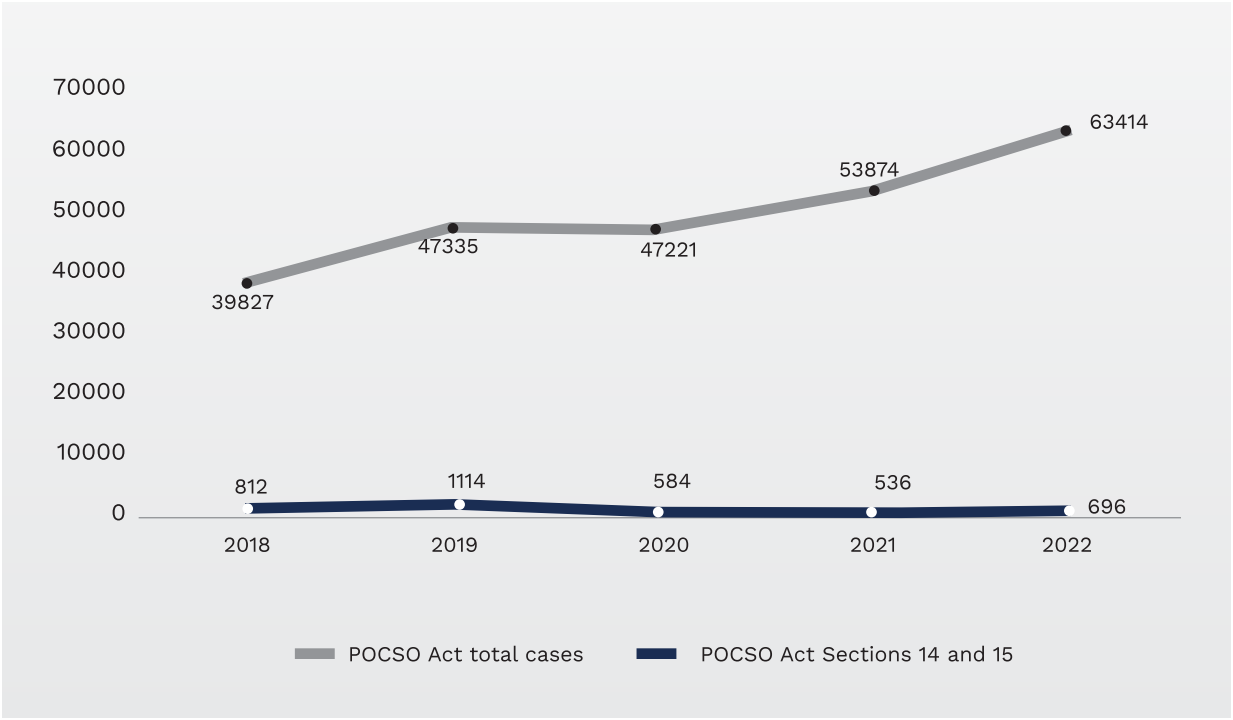
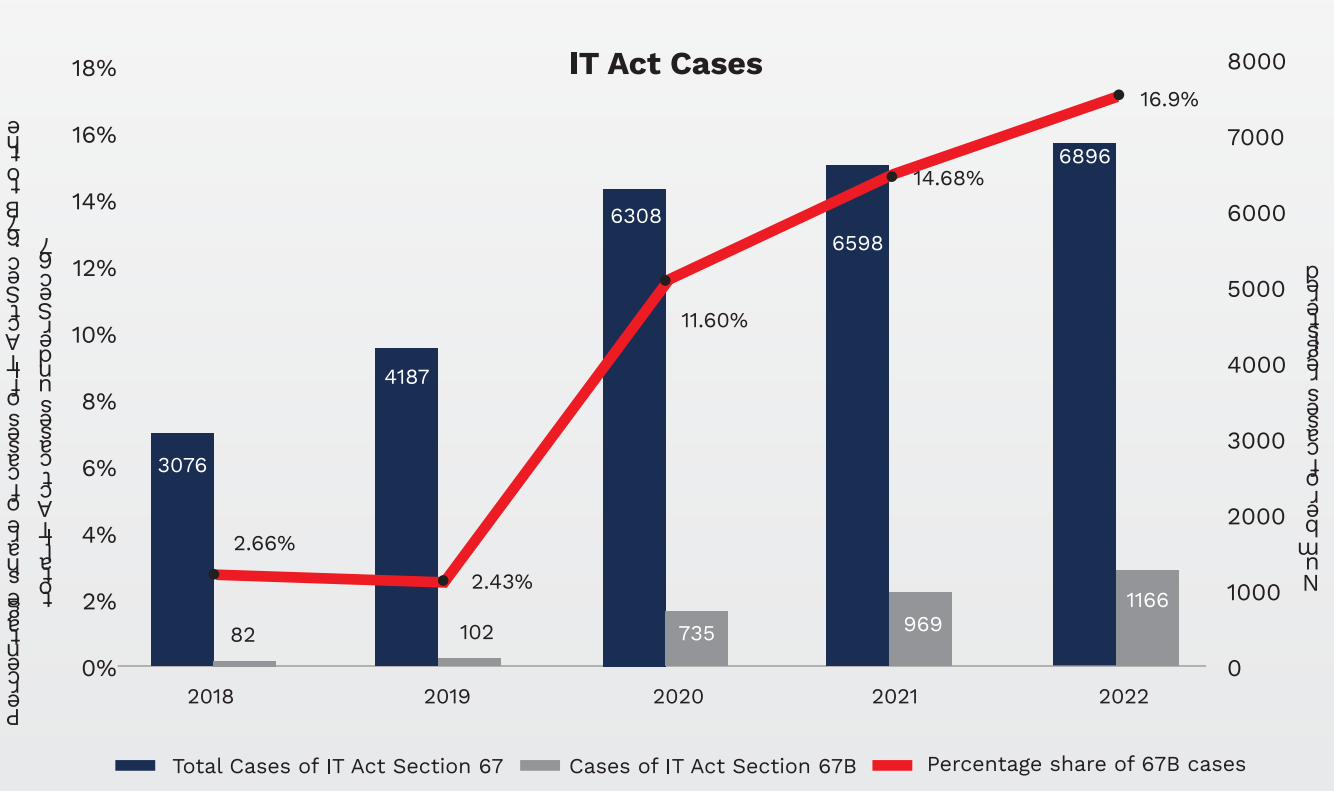


Figure 2 depicts that the number of cases registered under the IT Act Section 67B has been increasing in the last 5 years. It increased by 796 percent from 2018 to 2020 and 58 percent from 2020 to 2022. Among metropolitan cities, for which information is available, Delhi registered the most number of cases consecutively for two years i.e 154 in 2021 which constituted 16 percent of the total Section 67B cases registered in the country and, 116 in 2022, which constitutes 10 percent of the total Section 67B cases.

The percentage share of cases registered under Section 67B of the IT Act (cybercrime against children) to the total cases registered under the IT Act recorded more than five-fold increase during 2018-2022. In 2018, the percentage share was less than three percent which took a huge jump to 17 percent in 2022. This again highlights the fact that cybercrime against children increased substantially in India, especially after 2019.

Figure 2: Cases registered under IT Act (A), IT Act Section 67B (B) and percentage share of B to A



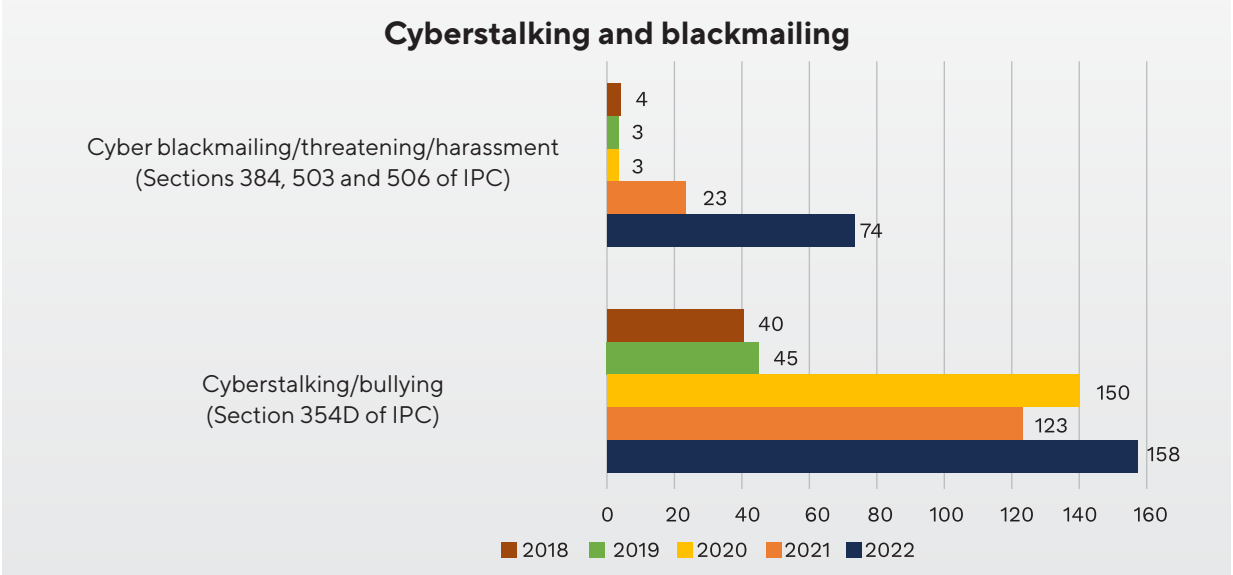
Note: The IT Act comprises all kinds of cybercrimes across the board. Section 67 of the Act refers to publishing and transmitting of sexually explicit or obscene images in electronic form. Within this Section is Section 67B which deals with cases involving children.

There are other cybercrime cases' data in the NCRB which might be worth noting. These crimes are not explicitly sexual in nature however, bullying, stalking and blackmailing can all lead to sexual exploitation and so, trends for these crimes are significant to this study. The lockdowns in India in 2020 and 2021 saw two very similar and disturbing incidents of bullying turning into crimes of sexual nature – Sulli Deals app in July 2020 and Bulli Bai app in January 2021 – where young perpetrators were seen putting up pictures of Muslim women without their consent in order to humiliate them by virtually auctioning the women through their images. These were incidents where women found themselves stalked, bullied and humiliated online (Dasgupta, Independent, January 2022).

Cyber psychologists saw a large number of online grooming cases during the pandemic where mostly an older man would try to groom young women and children in order to abuse them and extort sexual favours both online and offline. One such case was reported of a 15 year old girl who met an older man online offering her a modeling stint. They started talking regularly and he then confessed his love for her which she innocently believed. It started with him asking her to send him pictures of her face or lips but gradually went on to sharing of photos without clothes and in various positions/actions. The girl's siblings found out about it and contacted a cyber-psychologist who had to convince the girl that she was being trapped into a crime of heinous nature. This is one case of grooming but there have been many such cases that psychologists have encountered since the lockdowns in 2020 (Mehrotra, Scroll, September 2021). The offenders would usually confess their love, promise to marry the girls they are trying to abuse but ask them to keep the relationship a secret for some time in order to continue the abuse.

The number of cases registered under Section 345D of the IPC (cyberstalking) increased by 295 percent (40 in 2018 to 158 in 2022). The number of cases registered under cyber blackmailing/threatening/harrassment increased by 1750 percent (4 in 2018 to 74 in 2022).

Figure 3: Cases registered under cyberstalking and cyberblackmailing

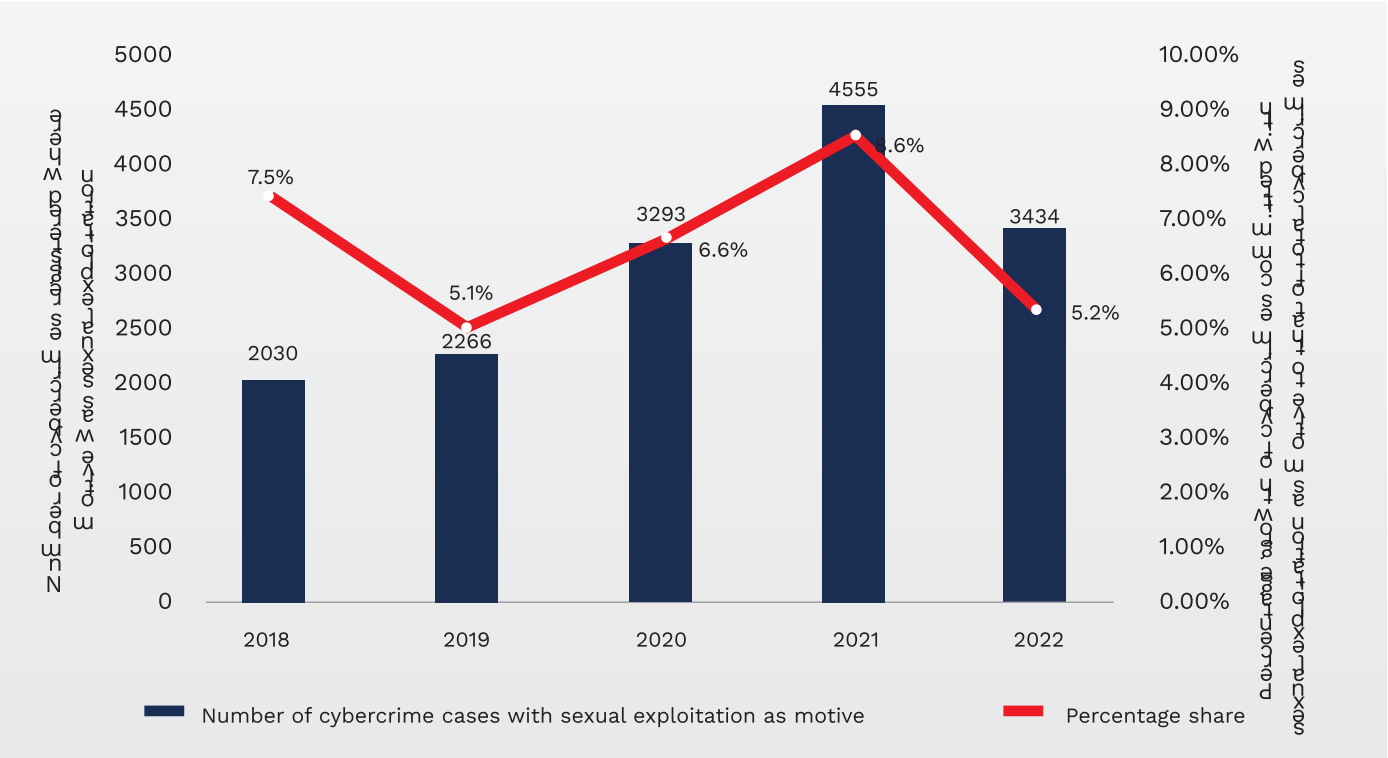


Sexual exploitation as motive for cybercrimes

While the percentage constitution of cybercrimes with sexual exploitation as motive vary a little every year, in actual numbers, the cases of cybercrimes reported to be for sexual exploitation are increasing every year (Figure 4). They fluctuate throughout the five years presented below but overall, increased by 69 percent in the last five years (2,030 in 2018 to 3,434 in 2022).

This data is not specific to children but also includes adults. The NCRB report does not categorise data on motive based on age or gender. It is still important to note that sexual exploitation is an important motive behind committing cybercrimes for offenders. Clubbed with other findings like ICPF's report, one cannot deny that many of these crimes are committed against children. Researchers on mental health have found time and again that sexual exploitation of women and children affects their mental health acutely. Victims of abuse have significantly higher rates of psychiatric disorders like anxiety, depression, eating disorders, PTSD. (Penza et.al., 2003 and Spataro et.al., 2004). Moreover, as has been mentioned earlier, cybercrimes are permanent in the sense that once an image or video is uploaded online, there is no way to find out who and how many people downloaded and shared it. This knowledge of an image of their abuse being out there in the world affects people and especially children. The fact that these crimes are increasing is an alarm for the society then.

Figure 4: Cybercrimes with sexual exploitation as motive



Note: The figures are not specific to children. It includes adults also

Disposal pattern of cases by police and court

The chargesheeting rate for cases filed under POCSO Sections 14 and 15 (about 75 percent) stayed relatively stable in 2021 and 2022. In terms of numbers, the cases chargesheeted under POCSO declined by 22 percent in 2021 as compared to the preceding year but increased by 42 percent in 2022. On the other hand, cases under the IT Act saw a 65 percent increase in 2021 and a 16 percent increase in 2022. The disposal of POCSO Act (Sections 14 & 15) cases witnessed decrease of 4 percent in 2021 but saw an increase of 40 percent in 2022. The same under IT Act (Section 67B) increased by 234 perecnt in 2022 which is substantially high. The overall disposal of cybercrime cases by the police rose by 15 percent 2022.

One main reason for the police not being able to close many cases is insufficient evidence which is an increasing problem with cybercrimes (Kancharla, Factly, January 2020).

The rate at which new and diverse methods of cybercrimes are being committed by offenders is much higher compared to the police being trained in investigating these crimes (Fourie, 2020). As can be seen in Table 3, the data of police disposal pattern in the last three years shows that the chargesheeting rates are very low for total cybercrime cases. Another reason for high pendency rates of these crimes is the absence of a comprehensive information-sharing model among the investigating agencies. Moreover, there is no standard procedure for searching or seizing digital evidence. On top of it, many officials don't even know their adjudicating powers under the IT Act (Saikia, Mint, July 2016). It is also important to note that the dark web is still a major mystery to us. Neither are children aware of the risks involved there, nor are investigating agencies prepared for the kinds of cybercrimes committed against children (Joy, Deccan Herald, June 2019).

Table 3: Police disposal pattern for cybercrime cases during 2020-22

Sl. No.		Total Cybercrime			POCSO Act (Sec. 14 & 15)			IT Act (Sec. 67B)		
		2020	2021	2022	2020	2021	2022	2020	2021	2022
i	Total cases of cybercrimes	103,988	127,330	138,767	1,257	1,199	1,324	831	1,417	1,986
ii	Cases disposed of by police	29,820	55,427	63,988	598	574	802	440	820	1,994
iia	**% Change in disposal**	**26%**	**86%**	**15%**	**-29%**	**-4%**	**40%**	**378%**	**86%**	**234%**
iii	Cases chargesheeted	14,176	18,744	18,925	537	421	596	272	450	524
iiia	**% Change in chargesheeting**	**53%**	**32%**	**1%**	**-28%**	**-22%**	**42%**	**377%**	**65%**	**16%**
iv	Chargesheeting rate	47.5	33.8	29.6	89.8	73.3	74.3	69.6	75.4	59.3

An important gap that can be seen from the court disposal data of cybercrimes is the unfortunate state of convictions of the reported crimes in courts. High pendency rates and negligible conviction rates only deter the public from believing that reporting such crimes would yield any result. This leads to under-reporting of cybercrime cases which is another problem. The percentage of cases that ended with conviction out of the total cases listed for a trial in 2022 is about one percent for the overall cybercrimes as well as cybercrime cases under POCSO (Sec. 14 & 15) and IT Act (Sec. 67B). A comparison od data from the last three years suggests that 2020 was an exception as the number of cases where the conviction made was substantially higher compared to 2021 and 2022.

Table 4: Court disposal pattern for cybercrime cases during 2020-22

Sl. No.		Total Cybercrime			POCSO Act (Sec. 14 & 15)			IT Act (Sec. 67B)		
		2020	2021	2022	2020	2021	2022	2020	2021	2022
i	Total cases for trial	40,656	54,979	66,765	1,314	3,065	3,530	438	888	1,397
ii	Cases disposed	4,420	7,139	6,685	82	131	119	2	15	45
iii	Cases convicted	1,110	491	1,118	63	35	29	-	7	19
iv	**% Conviction to the total cases for trial**	**2.7**	**0.9**	**4.8**	**4.8**	**1.1**	**0.8**	**0.0**	**0.8**	**1.4**
v	Pendency rate	**89.1**	**87.0**	**90**	**93.8**	**95.5**	**96.6**	**99.5**	**98.3**	**96.8**

Conclusion and Recommendations

From the literature, news, studies and data, it is clear that cybercrimes against children are on the rise and this is becoming one of the most important issues to tackle with since the internet is a world of not just knowledge but also entertainment which is equally important for children. The pace of the world has become extremely fast and to miss out on it is an unfair outcome for children. However, the crimes committed online against children not only reduce their experience of learning and entertainment but also have a huge effect on their mental health. The Internet appears to have entered our lives without really preparing us for its consequences and ethics and this incomprehensive nature of it affects children even more.

With the outbreak of the pandemic, the crimes committed online for sexual exploitation have increased, especially crimes against children for their gullible and trusting nature. Like the internet, the crimes are also ever-evolving creating an alarmingly unsafe space for children. The pandemic saw a new aspect to human trafficking – cyber trafficking – a crime that affects women and children the most. In five years, the percentage share of publishing and transmitting sexually explicit mateiral involving children to total IT Act crimes recorded a five-fold increase. Even total cybercrimes against children have increased 8 times in these five years. It is then an acutely important need of the hour to start working on reducing and eventually putting an end on cybercrimes immediately.

In this context then, what needs to be done to curb this growing menace and how to create safer and nurturing environments online for children? Some recommendations to do so are as follows:

1. Awareness programmes:

(i) For better reporting - Bridging the major gaps in awareness about legislations against child sexual abuse is important for more reporting of cybercrimes. Awareness generation around the online portals to report child sexual abuse is also important. Create awareness on the National Tipline for reporting of cybercrimes against children,

(ii) For children and caregivers – Schools are an important place where such awareness can be imparted through specific workshops targetting parents and children. Since children are not only exposed to content and contact risks but also conduct risks, they could be potential offenders themselves. A good educational workshop on online safety would not only target potential and actual victims but also potential perpetrators of online violence and this would be a useful tool. Creating awareness and tools which enables parents for early detection of accessing CSEAM content by children.

(iii) CyberPravah – The journal published by I4C, Ministry of Home Affairs is not available in the public domain. It is important for the public to know cybercrime trends in the country based on cases registered. It is recommended that the journal and its information be accessible to general public.

2. Legislative and measures: Robust

policies and legislative measures are the building blocks in protecting children from cybercrimes, along with the inclusion of broader definition of child pornography. Notably, among these are the need for amendment to both the POCSO Act 2012 and the IT Act 2000.

a. Amendment to the POCSO Act, 2012 to include the offence for advocating or counselling sexual activities with a person below 18 years through any written material, visual representation or audio recording or any characterisation.
b. Synchronous to this is an amendment to the IT Act, 2000 for punitive action for those providing pornographic access to children, and also those who access, produce, or transmit child sexual abuse materials.
c. Removal of CSEAM content by Intermediaries after getting information from appropriate government / authorized agencies should not be more than 6 hours, as against 36 hours under Rule 3 (1)(d) of the Intermediary Guidelines, 2021.
d. Accountability of institutions receiving actionable intelligence: This would enable intelligence sharing from international law enforcement to local law enforcement agencies/ police departments to ensure investigation.
e. Swift legal deterrance through investigation and disposal: Faster investigation and disposal of cases would provide the necessary deterrance. Since cybercrimes against children have increased so much, special attention needs to be given to this growing menace. Speedy trials and subsequent prosecutions could be a deterrent for current and future offenders.

3. Increased Nirbhaya Fund: Currently, only 3.61 percent (INR 224.76 crores out of INR 6212.85 crores) of the Nirbhaya Fund is disbursed to Cyber Crime Prevention against Women and Children (CCPWC). The appraisal of funds was done in 2016. Moreover, as mentioned earlier, till July 2022, 3.2 percent of the amount disbursed has been for CCPWC. However, cybercrime trends show that cybercrimes in general and especially against children have increased since the lockdowns in 2020 and children using internet more, thus making them vulnerable to crimes. It is then important to reconsider the allocation of funds and increase the amount for CCPWC keeping in mind the urgency of the matter.

4. Technology engineered safer platforms for children: Creating user platforms that are inherently safe for children's use is a growing technology all over the world. This essentially means that technology can be used to create platforms that exclude certain kinds of content, certain categories of users (adults, strangers), or certain problematic behaviour. Such platforms could create a genuinely safe and enriching experience for children devoid of exposing them to crimes and other vulnerabilities.

a. Amendments to the IT Act 2000: Internet Service Providers and online platforms' responsibility and accountability for ensuring safe internet access to children is an urgent need, especially since greater access and use of internet for children has been recorded since the pandemic. Amendments to the IT Act for making intermediaries responsible for all measures to proactively identify and remove CSEAM as well as report it to Indian authorities. Gateway ISPs must

bear significant liability to detect and block CSEAM websites.

5. National Task Force: One of the most important tasks afront us is to to develop a comprehensive and coordinated response of investigation and intelligence agencies to combat against online child sexual abuse. It is thus, recommended to develop a national task force which would:

(i) formulate a legislative and an administrative framework by defining and addressing all forms of sexual and non-sexual nature of digital or online abuse against children.

(ii) set a dedicated mechanism to strengthen the intelligence apparatus to improve the collection, collation, analysis and dissemination of operational intelligence from the organized crime perspective.

(iii) set up a National Tipline for reporting of child sexual abuse and cybercrimes against children, as well as distribution of CSEAM by children and concerned citizens.

(iv) facilitate inter-state transfer of evidences for investigation purposes, for cyber policing and with prosecution capabilities.

6. Collaboration between national and global law enforcement agencies: The national task force should also play an important role in;

(i) strengthening international cooperation with concerned law enforcement agencies, in developing intelligence for the purpose of investigation;

(ii) working towards developing offenders registry;

(iii) promoting bilateral or multi-lateral mutual legal assistance treaties to coordinate and conduct investigation where international ramifications of the alleged crime of online abuse children is reported or suspected;

(iv) facilitating universal action by implementing obligations under the various international conventions and protocols that are in force in respect of countering any kind of abuse against children, etc.

References

Akhawat, T. (2022, November 18). The deplorable world of child sexual abuse. *Deccan Herald*. https://www.deccanherald.com/opinion/in-perspective/the-deplorable-world-of-child-sexual-abuse-1163397.html.

Anand, A. (2022, June 25). Explained: The increasing rate of cybercrime in India. *CNBC TV18*. https://www.cnbctv18.com/india/cyber-crime-are-on-a-rise-in-india-amit-shah-cyber-security-ncrb-data-13913912.htm.

Basu, O. (2022, September 22). India witnessed 17-fold rise in child pornography cases, UP & Kerala on top. *Zee News*. https://zeenews.india.com/india/india-witnessed-17-fold-rise-in-child-pornography-cases-up-kerala-on-top-2512885.html.

Chang, L. Y. C. And Grabosky, P. (2017). The Governance of Cyberspace. In P. Drahos (Ed.), *Regulatory Theory: Foundations and Applications* (pp. 533-552). ANY Press.

Dasgupta, S. (2022, January 8). What is Bulli Bai scandal: Indian app that listed Muslim women for auction. *Independent*. https://www.independent.co.uk/asia/india/bulli-bai-app-arrests-muslim-women-b1988504.html.

Deora, R.S. and Chudasama, D.M. (2021). Brief study of cybercrimes on an internet. In *Journal of Communication Engineering & Systems 11*(1), pp. 1-6.

DNA Webdesk. (2022, September 26). Child porn, rape videos 'available freely' on Twitter, Delhi Commission for Women issues summons. *DNA*. https://www.dnaindia.com/india/report-child-porn-rape-videos-available-freely-on-twitter-dcw-chief-swati-maliwal-issues-summons-2986663.

Fourie, L. (2020). Protecting children in the digital society. In J. Gorebbelaar and C. Jones (Eds.), *Childhood vulnerabilities in South Africa: Some Ethical Perspectives* (pp. 229-272). African Sun Media.

Gasser, U. and Cortesi, S. (2017). Children's rights and digital technologies: Introduction to the discourse and some meta-observations. In M. Ruck, M. Peterson-Badali, and M. Freeman (Eds.), *Handbook of children's rights: Global and multidisciplinary perspectives* (pp. 1-45).

Halder, D. and Jaishankar, K. (2014). Patterns of sexual victimization of children and women in the multipurpose social networking sites. In C.D. Marcum and G.E. Higgins (Eds.), *Social Networking as a Criminal Enterprise* (pp. 125-144).

Harrison, C. (2006). Cyber space and child abuse images: A feminist perspective. In *Affilia 21*(365), pp.365-379.

Hindustan Times. (2021, October 19). Online searches for child sexual abuse content rose 95% in India during Covid-19. https://www.hindustantimes.com/health/online-searches-for-child-sexual-abuse-content-rose-95-in-india-during-covid19-101634663358782.html.

Joy, S. (2019, June 23). People, cops helpless as cybercrime goes out of control. *Deccan Herald*. https://www.deccanherald.com/specials/insight/people-cops-helpless-as-cybercrime-goes-out-of-control-742222.html.

Kancharla, B. (2020, January 24). In 5 years, more than fourfold increase in the number of pending cyber-crime cases. *Factly*. https://factly.in/in-5-years-more-than-fourfold-increase-in-the-number-of-pending-cyber-crime-cases-in-courts-the-police/.

Kellogg, S. (2020, September 15). POCSO Act: Only 13.7% TN children aware, Bihar has almost nil awareness. *The News Minute*. https://www.thenewsminute.com/article/pocso-

act-only-137-tn-children-aware-bihar-has-almost-nil-awareness-133077.

Krishnakumar, S. (2022, September 1). Cybercrimes in India rise 6% a year in 2021, Telangana tops list: NCRB. *Money Control*. https://www.moneycontrol.com/news/india/cyber-crimes-in-india-rise-6-a-year-in-2021-telangana-tops-list-ncrb-data-9115161.html.

Kumar, S. (2021). Crime against children in cyber world. In *Journal on Contemporary Issues on Law, 5*(9), pp. 28-36.

Martin, J. and Alaggia, R. (2013). Sexual abuse images in cyberspace: Expanding the ecology of the child. In *Journal of Child Sexual Abuse*, 22, pp. 398-415.

Mehrotra, K. (2021, September 18). In the pandemic, more Indian children are falling victim to online grooming for sexual exploitation. *Scroll*. https://scroll.in/magazine/1005389/in-the-pandemic-more-indian-children-are-falling-victim-to-online-grooming-for-sexual-exploitation.

Ministry of Women and Child Development. (2021, July 22). *Utilisation of Nirbhaya Fund*. [Press Release]. https://pib.gov.in/PressReleasePage.aspx?PRID=1737773.

Ministry of Women and Child Development. (2022, February 11). *Projects under Nirbhaya Fund*. [Press Release]. https://pib.gov.in/PressReleasePage.aspx?PRID=1797692.

Ministry of Women and Child Development. (2022, July 22). *Nirbhaya Fund*. [Press Release]. https://www.pib.gov.in/PressReleasePage.aspx?PRID=1843810.

Naidu, J. S. (2021, July 25). 215 FIRs lodged, 105 held for uploading child porn since Dec 2019. *Indian Express*. https://indianexpress.com/article/cities/mumbai/215-firs-lodged-105-held-for-uploading-child-porn-since-dec-2019-7420908/.

Narayan, V. (2022, January 3). Cybercrime against kids up 261% in 2020, 116 held, 1 convicted. *The Times of India*. https://timesofindia.indiatimes.com/india/cybercrime-against-kids-up-261-in-2020-116-held-1-convicted/articleshow/88655385.cms.

Narnolia, N. (n.d.). Cybercrime in India: An overview. *Legal Service India*. https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html.

Pandey, M.C. and Singh, D. (2022, September 24). CBI searches 59 locations across states over online child sexual exploitation material case. *India Today*. https://www.indiatoday.in/india/story/cbi-searches-locations-india-online-child-sexual-exploitation-material-case-2004212-2022-09-24.

Pandit, A. (2020, April 25). NCPCR issues notice to online platforms over child sexual abuse. *The Times Of India*. https://timesofindia.indiatimes.com/india/ncpcr-issues-notice-to-online-platforms-over-child-sexual-abuse-material/articleshow/75382041.cms.

Penza, K.M., Heim, C. and Nemeroff, C.B. (2003). Neurobiological effects of childhood abuse: implications for the pathophysiology of depression and anxiety. In *Archives of Women's Mental Health 6*(1), pp. 15-22. https://link.springer.com/article/10.1007/s00737-002-0159-x.

Raj, R. (2017, February 3). After cops fail, Kerala hackers declare war on Facebook porn. *Deccan Chronicle*. https://www.deccanchronicle.com/nation/current-affairs/030217/operation-big-daddy-by-kerala-cops-fails-to-check-spread-of-porn.html.

Saikia, A. (2016, July 29). Why most cybercrimes in India don't end in conviction. *Mint*. https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-

cyber-crimes-in-India-dont-end-in-conviction.html.

Sarma, A. (2022, June 24). A pandemic of abuse: How India is protecting its children online. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/how-india-is-protecting-its-children-online/#_ednref1.

Spataro, J., Mullen, P.E., Burgess, P.M. Wells, D.L. and Moss, S.A. (2004). Impact of child sexual abuse on mental health: prosepective study in males and females. In *The British Journal of Psychiatry: The Journal of Mental Science 184,* pp. 416-421. https://www.cambridge.org/core/journals/the-british-journal-of-psychiatry/article/impact-of-child-sexual-abuse-on-mental-health/1344FE166B2E094FADD37505687BFF41.

World Health Organization. (2022). *What works to prevent online violence against children?* Geneva: WHO Publications.

INDIA
CHILD
PROTECTION

W 33-34, Okhla Phase -2, New Delhi-110020, India
www.childprotection.org.in