Research Article

A Psycho-Legal Analysis of Cyber Behaviours of Children: Legal Responses to Online Delinquencies

Shivani Verma
Assistant Professor
Law Centre-I, Faculty of Law, University of Delhi
Email- shivanishini@yahoo.co.in

Manuscript Submission Date: August 30, 2025
Manuscript Acceptance Date: December 30, 2025

Abstract

The contemporary digital revolution offers an unprecedented avenue for global connectivity and learning for children, but it simultaneously exposes them to an insidious cyber vulnerability, including grooming, pornography, bullying, trafficking, and exploitation, ruining their innocence to a 'beyond-imagination' trauma. This research paper analyses the philosophical dimension of cyber behaviour, revealing the risks of identity crisis, psychological trauma and social withdrawal. The paper also analyses the online behaviour of children, including excessive screen engagement, limited social interactions and exploratory navigations, establishing how their innate curiosity leads them to the trap of the faceless online predators, harmful content and peer aggression in cyberspace, sometimes culminating in delinquent behaviours in them.

Cyberspace has a unique nature that has no borders or shape. Existing legal framework in India, like the Bhartiya Nyaya Samhita, 2023, the Protection of Children from Sexual Offences Act of 2012 and the Information Technology Act of 2000, provide a comprehensive deterrence, but fails to prove effective because of the enforcement gap, jurisdictional hurdles and lack of digital literacy and stringent judicial scrutiny.

Literature review also reflects empirical gaps due to scarcity of longitudinal data, rural under-representation and non-synchronised psycho-legal interventions. Drawing from the studies of on-screen induced behaviour and awareness model of Hinduja and Patchin (2024), this research paper suggests a multidimensional psycho-legal framework while effortlessly integrating the awareness and preventive education with therapeutic rehabilitation and technological reforms.

The paper proposes technology-driven innovative safeguards to protect children in cyberspace. The dual nature of cyberspace demands collective action from parents, platforms, lawmakers, enforcement agents and psychologists. Limited screen time with parental control and involvement of children awareness programs and digital literacy through schools and agencies like CBSE and NCERT, etc., can create a secure cyber. Proactive guardianship, harmonising technology, psychology and law can create resilience in the cyber-behaviour of children.

Keywords: Cyber space, Delinquencies, Psychology, Online-grooming, Pornography

Introduction

The digital revolution has steered an unprecedented opportunity for learning, articulating and connecting, globally. For children, the internet offers a vast world of exploration and imagination but within this virtual landscape, there is a dark, deep and insidious realm;

the area where the innocence of childhood is increasingly being exposed to manipulations, exploitation, trauma, and harm. As children's presence in the digital space is increasing so are their vulnerabilities as they expose themselves to a range of cyber-crimes including but not limited to online grooming, pornography, cyber-bullying, trafficking, sexual-exploitation and unintentional exposure to harmful content. The virtual vulnerabilities not only develop technological risks but they also throw profound legal and ethical challenges. Purity, innocence and dependence of a child become paradoxically empowered and endangered in cyberspace. Cyber-crimes leave emotional and cognitive impact on children and inflict a grave harm that extends beyond the screen and might result in long term psychological trauma, identity crisis and social withdrawals. The cross-territorial and faceless nature of internet-players challenges the traditional legal thought process and makes it imperative for the lawmakers to evolve in order to understand the new challenges and design laws in both substance and spirit to meet the demands of child protection in the digitalised world.

Bhartiya Nyaya Samhita, 2023 along with Protection of Children from Sexual Offenses Act (POCSO),2012, the Information Technology Act, 2000 in consonance with the United Nations Convention on Rights of the Child are the response to the growing concerns for child safety. However, the efficacy of these legal mechanisms remains questionable, due to challenges like; enforcement hazards, jurisdictional limitations and digital illiteracy etc. This research paper explores the philosophical foundation of child vulnerabilities along-with child protection in the digital era, while examining the existing legal response and attempts to propose a holistic approach that aligns technological advancement with ethical and social responsibility and the legal reforms, related thereto.

This research paper attempts a multidimensional analysis as it dwells deep into the psychology of children in cyberspaces. While identifying their inherent and emerging vulnerabilities, the paper critically analyses the existing legal mechanism, with a child-centric approach that explores the significant dimensions of legal protective mechanism, preventive education and psychological rehabilitation of the children in distress. The paper aims to construct the idea of a safe digital environment, with a responsive, compassionate system to uphold the mental well-being and holistic development of the children.

Literature Review

The growing presence of children in cyberspace has resulted into extensive scholarly research into the vulnerabilities that they face and the effectiveness of the legal and social protection mechanisms. The literature available reveals an intricate juncture between the psychological susceptibility online behaviours and delinquencies and the legal framework for protection of children in digital surroundings.

Cyber Behaviours and Psychological Vulnerabilities

Researchers connect the online experiences and risks to the children's cognitive and emotional development. Hinduja and Patchin (2024) in their book, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (3rd Edition, 2024) believe that adolescents' behaviour to explore in combination with lack of digital literacy increase their susceptibility to the crimes like cyber bullying and exposure to inappropriate contents. Further the psychological impact of victimisation manifests

into anxiety, depression and in most extreme cases, self-harm.

Brown (2017) in his book *Online Risk to Children: Impact, Protection and Prevention* analyses how the permanent and public nature of the online environment uniquely aggravates the trauma and leaves an eternal psychological scar on the child. Rajput et al. (2024) Emphasises how Covid 19 pandemic amplified vulnerabilities in children by increasing their online time and elevating the chances of exposure to cyber risks. In his book *Online Child Sexual Abuse: An Indian Perspectiv*e, he tries to break new grounds in the discourse of child sexual abuse material and the online victimisation of the children specifically in Indian context. The book explores the case studies forensic digital technologies and provides a valuable analysis of legal inadequacies and procedural hurdles in Indian cybercrime enforcement systems.

Child Protection Mechanism: The Legal Response

India the legal mechanism has evolved tremendously in response to the surge of cybercrimes against children and yet the challenges persist. Laws like the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000 are the legislative efforts to prevent cybercrimes and to protect children. Karnika Seth (2015) in her book Protection of Children on Internet, highlights the enforcement hurdles and analysis jurisdictional complexities and limited digital literacies as their reasons that the laws are not fully efficient to deal with the menace.

Legal studies by Milosevic (2018) and Elshenraki (2020), underscore the global nature of the issue and hence stress upon the need for international legal framework cooperation and a universal collective attempt to combat cybercrimes against children. They also highlight the dappled accountability mechanisms within the social media platforms and hence call for enhanced child centric governance models regulating the social media platforms and keeping a check on them. Tijana Milosevic in his book highlights the role of social media companies and blame their inconsistent protections standards as one of the reasons that the cyber-crimes are so rampant in the society.

Hossam Nabil Elshenraki (IGI Global, 2020) talks about the growing threat of online exploitation of children including pornography and trafficking etc. He adopts a global multi agency perspective and calls for an integrated action from the society as whole including; the law enforcement agencies, educators, and civil society.

Integrating Therapeutic and Preventive Strategies: A Profound Gap in Literature

There is a gap within the literature specifically related to the holistic approach combining with the legal actions, psychological rehabilitation and preventive education. Developing safer Online Environment for Children (Information Resource Management Association, 2019) emphasises legal response including policies for digital resilience and emotional support to nurture safer online spaces. Similarly, Hinduja and Patchin's (2024) work also highlights the importance of awareness in children, parents, and educators so that a collective intervention alongside with the legal protection can address the root cause of the vulnerability and protect the children in real sense.

The body of literature available collectively highlights the complexity of cyberspaces-vulnerabilities in the children and reveal a need for a multidimensional approach. Legal frames provide a crucial protection but

still most of the literature proposes for complementary psychological and educational intervention so that resilience and holistic well-being of the children can be fostered and ensured. However, the legal framework in India tries to provide a crucial protection to children but most of the available literature proposes only supplementary educational interventions and psychological understandings to foster holistic well-being of children and nurture resilience in them. The literature available, attributes the inefficiency of law enforcement machinery to digital illiteracy and jurisdictional blogs but fails to propose any effective suggestions.

This research paper attempts to synthesise a psycho-legal perspective by proposing a compassionate child centric system attuned to the digital age challenges.

Research Questions

1. What are the behavioural foundations of children's vulnerability in digital space, and what harm do they manifest psychologically, emotionally, and socially?
2. How effective is the legal framework in India to deal with cyber delinquencies and to protect children in cyberspace?
3. What child centric strategies including; awareness, preventive education, psychological rehabilitation, and legal reform etc. are adopted in India to ensure safe digital environment for children?
4. How effective will a holistic multidimensional approach integrating law, psychology, and technology will be to ensure holistic development and mental well-being of the children, online?

Methodology

A qualitative, doctrinal and interdisciplinary methodology based on legal and psychological analysis is adopted for the purpose of this research. The study inherently requires a nuanced and conceptual engagement with digital behaviour, child psychology, law and governance.

The legal analysis is done using doctrinal methods wherein statutes case laws international instruments and policy documents are thoroughly examined to understand how the law is conceptualised to respond to the cybercrimes against children. The Primary sources of law included for the purpose of this study are: Constitution of India, the Protection of Children from Sexual Offenses Act, 2012, Information Technology Act, 2000, Bhartiya Nyaya Samhita, 2023 and the United Nations Convention on Rights of Child etc. As secondary sources commentaries, books, psychological literature and child development theories are assessed and analysed

Selected case laws from the Indian and international courts have been thoroughly scrutinised to understand the judicial response to online child exploitation, which included an examination of judicial reasoning, sentencing patterns, interpretations related to the rights of child and freedom of expression, online on social media platforms. A normative and prescriptive perspective is used to critically evaluate the efficiency of the existing legal framework while proposing a multidimensional model for child protection.

It is a non-empirical qualitative study in nature and hence does not involve primary data collection and is limited to

secondary sources but aims to provide a deep theoretical insight and policy-oriented recommendations.

Online Behaviours of Children and their Vulnerabilities: A Psychological Exegesis

The current digital prominence has fundamentally reshaped the childhood and has embedded our children in a virtual world that influences Their gross. Online platforms often offer many educational and other benefits but at the same time they pose certain serious psychological and legal risks. A child's cognitive immaturity and his not-so-fully developed emotional mind, makes him vulnerable to exploitation and east prey of cyber-crimes. It is very important to understand behavioural patterns of children while interacting on digital platforms, in order to develop an effective legal strategy to protect the children and provide them the required therapeutic support.

Internet Usage

Increased digitalisation of society reflects in early engagement of children with the Internet which involves watching educational content to participating in multiplayer games and gradually exploring social network platforms, expanding and leaving digital footprints.

For children, Internet is an academic tool and a playground where they often engage without fully comprehending the implications of their engagements and actions. A child's behaviour on Internet can be categorised as passive consumption, wherein, he watches the videos or listen to the music and active engagement; wherein, he involves in posting the content, chatting gaming etc. And children, being the naïve beings as they are, most of the times imitate the trends blindly, accept friend requests from the strangers, explore the restricted content due to curiosity, fall for the peer pressure and enter into the zones, which are forbidden for an underdeveloped mind of a child. This indiscriminate engagement unfortunately exposes them to the bigger risk of cybercrimes, which further aggravate due to the absence of adult supervision or adequate digital literacy. What begins with harmless browsing might quickly evolve into a dangerous online experience due to lack of filters and foresight in a child.

Online Vulnerabilities

Developmental psychology asserts that children are inherently more vulnerable due to their immature cognitive and emotional faculties as compared to the adults. Hence children are more likely to misjudge a situation, fail to realise manipulations and act impulsively. Sometimes impulsive actions might involve oversharing of the personal information or engaging with the strangers online. Sometimes the approval of peers led them to follow or participate in a dangerous trend online. The inability to navigate or assess the harmful experiences like humiliation or manipulation online result into guilt, long-term anxiety, trauma, loss of focus in studies, hiding from or telling lies to the parents and in extreme conditions even legal delinquencies. The Internet which ideally should support learning and creativity can hence become a destabilising influence upon the children without appropriate psychological safeguards.

Psychological Impact on Children

Negative online experience can be profound and long lasting leading to serious mental health outcomes and sometimes children might also get

involved into illegal activities. Socially victims of cyber-crimes withdraw themselves socially, disengage academically and become very distrustful adults. The invisibility of Internet players intensifies the risk and the impact the permanence of online content aggravates the trauma further as the harmful material can be spread indefinitely and with infraction of seconds. Naive mind of a child experiences difficulty in distinguishing the virtual from the real. Without proper intervention the psychological scars of cyber-crime can persist into the victim child throughout his life making him emotionally unstable and sometimes a victim becomes the perpetrator wanting to repeat the cycle of harm.

Digital Addiction

Digital addiction is another concern particularly among children and adolescent which establishes after excessive use of online platforms and gradually convert into behavioural addiction which may be defined as a compulsive urge to use digital platforms despite harmful consequences. Children who are digitally addicted display withdrawal symptoms when they are denied the excess and experience a lack of interest in the real-world interaction. They also reflect anxiety, irritability, and aggression. Lack of sleep patterns, hygiene and poor academic interests, might lead such children into a situation, wherein, breaking law can also become a handy option for them. Digital addicted children isolate themselves socially and communicate less with the family which increases the risk of their engagement into forbidden activities and therefore digital addiction is not just a medical or behavioural issue but a societal challenge which needs thoughtful response from family and institutions.

Vulnerabilities and Risk Factors

While all the children are vulnerable to the online risks certain groups of children are significantly more at risk due to underlying psychological or socioeconomic factors like the ones having history of abuse neglect or trauma. Children with developmental disability, mental health issue or special educational needs lack cognitive capacity to detect and avoid online risks. Children from economically disadvantaged background may access the Internet in an unsupervised way or they may use a shared Internet which might expose them to the content which is not age-appropriate resulting into risks. If parents lack digital literacy children often receive no guidance or support and hence are more vulnerable to online risks. Factors like peer rejection, academic stress, a lack of attention from the parents, absence of friends, can lead vulnerabilities in children which might resulting into making them prime targets of cyber-crimes.

Latest Behavioural Trends and Emerging Risks

Cyberspace is increasingly becoming sophisticated and psychologically manipulative. Sextortion, for example, which involves coercing the minors to share sexually explicit content which is later on used to blackmail them or sexually exploit them. Online grooming that occurs for weeks or months, with the criminals building trust, in the children, then exploiting them, emotionally and sexually. Some children are lured into dark web, where they unknowingly interact with illegal or violent content, while others are lured to do the viral challenges like the 'Blue whale' or 'Momo challenge', pushing the vulnerable children towards self-destruction and suicide.

These platforms have no boundaries and their faceless nature makes it difficult to trace them or to prevent harm. Hence, these emerging trends call for immediate and coordinate responses from psychological educators, parents and legal reformers.

Recent Empirical Studies on Child Behaviors in Digitalspace: An Analysis

A cross-sectional survey in Northern India[1] revealed an average daily screen exposure of 70 minutes in children between six months to five years of age, with surprising 61% of the beginning of the use of the digital screens before the age of two years. Predictions encompass the age of the child screen habits in the household and lack of parental care, as the reason.[2]

A study in Ujjain identified more than two hours per day of screen time habit prevalent in the age groups between 3 and 15 correlating it with the decrease in physical activities and increase in sleep issues concerns related to eyesight and frequent headaches.[3]

Excessive use of screen links to certain risks related to behaviours in the children under the age of five including emotional instability and social deficit.[4] A study of 2025 which reviewed twenty-five different social experiments in India connected social media usage directly to Parenting and establishes weak parent child dies in the families where there is excessive screen exposure. This also results into obesity and mental health issues.[5] Studies also reveal that there's a risk of autism spectrum disorder among the toddlers using all their time in front of the screen instead of occupying their minds into more holistic development generating activities.[6]

Digital Addictions and Legal Delinquencies

Digital era has made screens and ubiquitous companion of children. From smartphones to gaming consoles, digital technology has brought entertainment knowledge and connections in our hands, but it has also exposed our children to serious psychological and behavioural risks. Children are not just consuming the digital content; they are deeply immersed deep in virtual world, to an extent, that their perception of reality, morality and consequences of their action; has distorted completely. A harmless engagement in digital world can spiral quickly into digital addiction which is an intense and compulsive dependence on screen that takes a child away from his normal functioning. Such exposure sometimes, might result into alarming repercussions, linked to juvenile delinquencies and criminal behaviours.

Children glued to their screams lose control on their emotions and social responsibilities as they start exhibiting signs of dishonesty, defiance and aggression. In India many cases have been reported, where children have resorted to steal money for in-game purchases, lied to their parents, skipped school, and even engaged in cyber bullying and digital frauds. The digital realm; while offering limitless entertainment and engagement; lacks the structured moral boundaries, which is very important for the children, during their formative years. Without

1 Unveiling Screen Time Habits: A Study on Digital Behavior of Young Children in India, 2025 S. Asian J. Soc. Stud. & Human.
2 Ibid.
3 Prevalence and Determinants of Excessive Screen Viewing Time in Children Aged 3–15 Years, PMC (2023).
4 Assessment of Risk of Behavioural Problems in Children Below Five Years in Relation to Screen Time, Cureus (2024).
5 Impact of Social Media on Parenting Style and Child Behavior in India: A Systematic Scoping Review, 2025.
6 Impact of Screen Time and Occurrence of Autism Spectrum Disorder among Toddlers, JCDR (2025); Do Children Need Humans or Screen?, 2023.

any correct guidance and regulation children are reported to have been engaged into extreme incident of committing acts of violence and crimes.

Some of the alarming incidents of delinquency reported in India in recent times are:

On 25th August 2025, the Times of India, reported two incidents which reflects, the impact of digital exposure and addictions.

First incident was reported of a 13 years old boy in Ahmedabad, who stole a phone and Rupees 1000 to be a YouTube gamer, when his mother denied him the access to the phone. Upon confiscation of his phone, he skipped school for days and threatened to commit suicide after which a counselling session was arranged through a helpline. He skipped school for days and, upon confiscation of his phone, even threatened suicide. Counselling was later arranged through a helpline. Second incident was of an 18 years old boy from Azamgarh, studying in class 12, committed suicide on 21st August 2025. In his suicide note, he mentioned gaming addiction and academic pressure as the reason of suicide. Moments before his death, he also asked to play 'one last game'.

In another alarming report published on 20th August 2025 in the Times of India, some of the renowned doctors highlighted surge in virtual autism among the young children due to excessive screen time. Doctors like; Dr. Lokesh Lingappa, a paediatric neurologist at a private hospital, Dr. Hemnath S., a neurologist at Osmania General Hospital and Dr. Dinesh Kumar, a neurologist at Gandhi Hospital corroborated that symptoms like; delayed speech or social interaction and emotional withdrawal is seen in very young children due to prolonged gadget use.

On 30th September, 2023 Dahod police in Gujarat reported a case, where a minor spent Rupees 13 lakhs from his grandfather's bank account, fraudulently, to fund his online-gaming and buy an expensive smart phone.

As reported in the Ahmedabad Mirror on 4th September, 2019, Maya Tripathi, Ahmedabad Child-Line Coordinator said that they had received 15 cases of complaint of excessive mobile use within the time period of one and a half year. It was further reported that city hospitals were also receiving at least 50 cases per month where kids needed intensive psychological counselling or treatment for being hooked to their screens and as a result developing violent behaviour and threatening to cause self-harm whenever asked to give away their screens.

On 7th July 2025, another case was reported in the Times of India. Surat Cyber Crime Cell registered numerous complaints under the Information Technology Act, 2000. In one such case, a minor boy used his mother's phone, given to him for online study, created a fake Instagram account by using another girl's identity and morphed her pictures inappropriately, committing cyber harassment. In another case police arrested a group of people including a minor in Nagpur. In order to showcase their lavish lifestyle online, they stole motorbikes and posted the reels on social media.

In *All India Gaming Federation v. The State of Tamil Nadu*[7], while discussing the constitutional validity of the Tamil Nadu Prohibition of Online Gaming and Regulation of Online Games Act of 2022 the honourable High Court expressed its concern for the users of the online gaming platform. The court said that the unchecked online gaming was causing online gaming addiction, which was

7 All India Gaming Federation v. The State of Tamil Nadu, W.P. Nos. 13203 of 2023.

further leading to financial distress for the families, sustainable debts, incidents of suicide, incitement to squander money. The users were also exhibiting psychological and physiological disorders as poor eyesight, reduced concentration, decreased productivity, diminished analytical thinking and aggressive behaviour, specifically in the young not-fully developed minds.

In *Amit Nair v. State of Gujrat,* AIR Online 2020 GUJ 2072, the court established a similarity between the Internet gambling and the traditional gambling activities. The court stated that they both raise same concerns including; possibility of fraud, conflict between the state and centre regulatory authorities, and a likelihood of addiction. The court also asserted that the questions of morality is pertinent in connection with Internet gambling and its accessibility to the children because in present times children are given unlimited access to the computers and Internet. The code further stated that it is a possibility that without proper monitoring children might access to gambling website and could come across indecent materials.

In *Play Games 24X7 Private Limited v. State of Tamil Nadu*, W.P. Nos. 6784 and 13158 of 2025, the court highlighted Article 39 of part four of the Constitution of India wherein indirect principles of state policy it is the responsibility of the state to ensure that the health of the children is well taken care of and they are given opportunities and facilities to develop in a healthy manner. Therefore, the Court emphasised that online games must not be available for children below the age of 18 years and must be played only by the persons who are 18 years and above and not school children.

M/S SBN Gaming Network Private Limited v. State of Chhattisgarh[8], is another case, where the court held that there has to be a difference between skill-based games and chance-based gambling. It is important for the gaming websites to understand the difference and develop the game's strategically so that the games which are made for the minors, do not expose them to any gambling platform and help them own their skills in a productive way.

Legal Response

In present evolving digital landscape of India children are increasingly exposed to online platforms where this connectivity although offers numerous benefits but it also brings along significant risks of children being exposed to cyber-crimes. Law in India recognises such threats and has adapted a protective mechanism for children in cyberspace. The Legal Framework in India aims to regulate digital behaviours, create accountability for digital platforms, penalises the offenders and provide redressal. The goal at large is not only to punish the wrongdoers but also to encourage responsibility and provide children the kind of protection they need while interacting in the virtual world. Few of the laws against cyber-crimes are discussed here.

Bhartiya Nyaya Sanhita, 2023

The Bhartiya Nyaya Sanhita, which replaced the colonial-era Indian Penal Code in 2023 addresses a lot of contemporary and new age concerns, including; the growing threat of online offenses against children. It recognises an urgent need of an extensive combat mechanism to fight digital exploitation of the children.

Section 128 of BNS condemns online sexual exploitation of children and explicitly criminalises exploitation of children through online means,

8 M/S SBN Gaming Network Private Limited v. State of Chhattisgarh, WPC No. 2515 of 2025.

including; online grooming, sending sexually explicit material to the children, requesting or coercing children to send sexually explicit or intimate photographs or videos, or engaging with or producing or storing any sexual abuse material over the Internet. Any such act is stringently punished with imprisonment and/or fine, depending upon severity of the offense.

Section 95 condemns the crimes of using children in digital criminal acts. The law makes it a punishable offense to use or hire a child to commit any crime; hence it would include involving children in the digital crimes. This provision can safeguard the children from being manipulated or coerced into participating in online crimes either as the victims or accomplices. Section 396 of BNS empowers the court to award appropriate compensations to the child victims of online offenses, so that, their rehabilitation can be supported.

The Information Technology Act, 2000

The Information Technology Act of 2000 was designed to address cyber related issues in India as it governs many digital concerns including cyber security and online safety. The act plays a vital role in safeguarding the children who are increasingly active online and hence prone to digital harm and other cyber-crimes. Section 66 E provides punishment for the violation of privacy ensuring safety from the instances where minors are secretly filled and pictured without their consent or knowledge. In context of cyber bullying and non-consensual content sharing, this section is very important.

Section 67 further criminalises publishing or transmission of any obscene material in electronic form. Section 67A and B address more grave forms of digital exploitation. While Section 67A focuses upon sexually explicit content in general section 67B targets specifically the child sexual abuse material (CSAM) and penalizes not only its creation but even its distribution and viewing. This section is very important in context of protecting minors from the online predators and from creating or sharing explicit content online.

Another worth mentioning provision is section 69 A which grants the government a power to block the access to harmful online content in order to uphold public safety and public order; like in the case of Blue Whale Challenge, that pose serious threat to children's mental health.

Intermediary guidelines were framed under the Information Technology Act in the year 2021, which further strengthened the provisions, for ensuring safety of children in cyberspace. These rules mandate that all the digital platforms like; Instagram, You-tube, and Facebook etc. and all the gaming apps, must remove the child sexual abuse material within 24 hours of receiving any complaint, related thereto. The platforms are also required, under the guidelines, to implement an AI-based content moderation mechanism and a policy for an age-appropriate excess feature along-with an option of parental control. They must also focus on appointing grievance redressal officers for quick and speedy redressal. Together, these provisions aim to ensure that children are safe in cyber-space by creating a safer and more accountable digital environment in India.

Protection of Children from Sexual Offenses Act, 2012

Initially the act was enacted to deal with sexual offenses committed against children and penalised the offenders of such sexual offenses. While conventionally the legislation was applied in cases involving physical sexual abuse of the children, with time

it has been recognised as a strong legal instrument, that can effectively be utilised to ensure safety of the children in cyberspaces also tackling the online sexual exploitation of children. Section 11,12 or 13, depending upon the gravity and nature of the offenses, can be used for the crimes like; sending sexually explicit messages, videos or images to the minors using Internet. Section 11 defines 'sexual harassment' in a wider perspective and includes online acts like; sending inappropriate text or engaging in sexually explicit or suggestive chat with a minor in the purview of sexual harassment.

Section 12 provides punishment for the sexual harassment of children and section 13 stringently addresses, depiction of children in pornographic content. As these offenses usually occur in digital environment, POCSO becomes a critical statute in combating online sexual abuse of children along with, the Information Technology Act of 2000. Section 14 and 15 of the Act provide punishment for the use of children in pornography and storage of such content even storing or viewing any kind of child sexual abuse material is punishable.

Online grooming is one of the cyber-crimes, which is the most rampant in minors, specifically the adolescents. It is an act of building trust with the minors, using digital platform, with an intention to sexually exploit them later, and such online grooming is punishable under POCSO. Online grooming mostly happens through gaming portals, chats or even through direct messages and children being the innocent ones cannot comprehend manipulation and often fall prey of these tactics. The Act allows a quick legal action before such abuse escalates into any physical or other kind of abuse, timely preventing, any further harm and penalising appropriately.

Juvenile Justice (Care and Protection of Children) Act, 2015

Juvenile Justice (Care and Protection of Children) Act, 2015 Is a legislation which primarily aimed for the welfare of children who are either in conflict with law or are in the need of care and protection. In today's digital context, it plays a vital role in the situations related to digital behaviour of children specially in the instances, lead the children to digital addiction or exposure and other kind of unlawful activities.

The actor recognises vulnerabilities in children and the behaviours generated out of such vulnerabilities; which, in digital context, can be categorised as; aggression, cyber bullying, online fraud, identity theft, or theft committed to fund digital addictions, like; in-game purchases or logging in charges of the paid apps. According to the mandate of this law, the children, who misuse digital platforms or get involved in any kind of criminal activity, due to the influence of digital content, are not held accountable in a juvenile context and are also treated through counselling while providing them appropriate rehabilitation. The act is inherently corrective and focuses upon reintegration of the children instead of punishment. The Act supports interventions including; behavioural therapies, skill building programs and awareness programs for children, specifically those who show signs of digital dependency and reflect any kind of criminal tendencies, triggered due to online influences.

Information Technology Act, 2000 along with Protection of Children from Sexual Offenses Act, 2012 and the Juvenile Justice Act, 2015; provides a multidimensional and holistic approach in response to both victimisation of the children and to treat the delinquencies, if any, is in digital premises.

National Cybercrime Reporting Portal

The Ministry of Former Affairs launched a National Cybercrime Reporting Portal that is https://cybercrime.gov.in. It is an important step in the process of strengthening digital safety in India specially, amongst children who are the most vulnerable to the cyber threats. The online platform allows the victims or their guardians to report all the categories of sexual cyber offenses including; online grooming, sextortion, exposure to inappropriate or harmful content, pornography and cyber bullying, The portal has a steadfast category for 'cyber-crimes against children', to prioritise and trigger a quick action by appropriate law enforcement agencies for child protection. It also offers an extensive guidance; as to how to reserve evidences, and how First Information Reports that is FIRs can be filed in the crucial cases, which involve children. The portal plays a vital role in bridging the gap between the real-world law enforcement and digital incident, making it easier, for the parents, children and teachers to seek help when children are targeted online.

NCERT and CBSE Guidelines on Digital Safety

Both NCERT and CBSE have recognised the psychological impact and behavioural reflections of excessive screen usage in children. They have issued extensive and multiple advisories in order to create digital hygiene and provide digital safety along with bringing awareness about safe online behaviours. The guidelines emphasise upon the need of digital literacy and asserts to make it part of the school curricula, so that the students can be engaged and encouraged to critically evaluate, the available online content and understand the risks, associated to it. Awareness and mindful evaluation of the content can make the children realise and recognise potential threats like phishing addiction or grooming etc. Through various advisories, the NCERT and CBSE have urged the teachers and the parents, to monitor the screen time, content that is being consumed by the children and to maintain an open communication with them. They are also advised to report suspicious online interactions promptly to avoid any kind of aggravation. The boards promote responsible Internet use through educating the children, so that they are not indulged into excessive sharing, are able to avoid suspicious links, and learn to be respectful on social media platforms. Building digital resilience in children from a very young age can equip them with the awareness and skills to navigate the Internet safely and be benefited by it.

Digital Personal Data Protection Act, 2023

The Act is a recent landmark legislation that aims to regulate the storage, collection and processing, of personal data in India. The DPDP Act introduces specific protections for children's online safety, while acknowledging; the vulnerabilities and excessive risk that children face in cyberspaces. The law makes it mandatory for online platforms to obtain verifiable parental consent before processing any personal data of a child under the age of 18 years. This includes the data, which is collected during the signing-up on any website, gaming apps, educational tools or social media platforms. The Act also expressly restricts all the platforms from engaging into any kind of behavioural tracking or targeted advertising specifically aiming at children thereby protecting them from manipulative digital marketing practices.

It furthermore empowers the users with the right to correct access and erase

their personal data at any point of time. If a platform violates these guidelines; in order to ensure their accountability in the digital ecosystem, the law provides strict punishments. In today's time when children are increasingly engaged with technology without fully comprehending and understanding the long-term implication of sharing their personal information this law is specifically very important. The Act strengthens privacy and supports a closed and safe online environment for children by regulating how their data is collected and used.

Judicial Response

Judges, in India, have played a vital role in combating cybercrime against children through protective and progressive judgements. The law has been interpreted with a child-centric approach, reaffirming the need for stricter penalties for online exploitation of children. Courts have also emphasised upon the importance of safeguarding the rights of children, in the digital space and need of harmonisation of national and international legal framework, so that a collective and more efficient mechanism can be derived for cyber-crimes which are transnational in nature. Through judicial pronouncements the courts have contributed in shaping the legal standards and prompting the legal reforms. Children are recognised as vulnerable community and judiciary has ensured that their best interest remains paramount while proceeding for cyber-crimes.

In *Just Right for Children Alliance v. S Harish*,[9] the honourable Supreme Court held that Madras High Court's interpretation that mere possessing or viewing child pornographic content cannot be punished under the Protection of Children from Sexual Offenses Act of 2012 is to be over-rules as, "The mere act of storing or viewing Child Sexual Exploitation and Abuse Material (CSEAM), even without distribution or transmission, constitutes an offense under Section 15 of the Act of 2012." The court further clarified that Section 15 punishes even the passive consumption of CSEAM and aligns with the international obligations under the Convention on the Rights of Child of 1980. The court also emphasised that the intermediaries like; a website or social media platforms, cannot invoke, the safe harbour and get protection under Section 79 of Information Technology Act of 2000 while, they fail to act against any known CSEAM content. The honourable Court gave extensive directions to the Union of India (Ministry of Women and Child Development) and to the courts, in para 260 of the judgement;

- Parliament is directed to bring an amendment in POCSO and substitute the term child pornography with child sexual exploitation and abuse material (CSEAM) so that it reflects the reality of such offenses more accurately.
- It was suggested that courts must note that the term child pornography must not be used in any judicial order and instead of it the term child sexual exploitation and abuse material (CSEAM) should be endorsed and used appropriately.
- The court further suggested to implement comprehensive sex education programs including information about the ethical and legal ramifications of child pornography to help creating a determent for potential offenders.
- It was also suggested that for the offenders, a rehabilitation program should be derived, while victims must be provided with an effective support service which might

9 Just Right for Children Alliance v. S Harish, (2024) 14 SCC 318

include therapeutic interventions, educational support, and psychological counselling etc.

- Court stated that for the offenders who are involved in viewing or distributing child pornography, CBT can be an effective mechanism for addressing cognitive distortion that triggers such behaviour.
- Focus was laid upon therapy programs for developing empathy and understanding the harm that is caused to the victims.
- Court further emphasised that raising awareness about the child's sexual exploitative material and its consequences can help in reduction of its prevalence, by destigmatising the reporting and encouraging the vigilance.
- It was asserted that a coordinated effort, collectively by various stakeholders like; health-care providers, law enforcement and child welfare services, educators etc. It can be used to identify at-risk individuals and for implementing intervention strategies for children, especially adolescents, with problematic sexual behaviours (PSB).
- The court reiterated that schools play a very crucial role in identification and intervention at early stages and hence it is important to implement curriculum-based programs to educate students about healthy relationships consent and appropriate behaviour in order to prevent PSB.
- Court directed Union of India that it may constitute an expert committee to devise a comprehensive program and mechanism for health and sex education for children and for raising the awareness about POCSO in order to create a robust approach for child protection and sexual well-being.
- And finally, Parliament was urged to consider making amendment in Section 15 sub-section (1) of POCSO to make reporting of online portals and instances of possession, storage and transmission of CSEAM more convenient and prompter for the general public.

In the case of *Central Bureau of Investigation v. Anurag Sharma*, CBI,[10] the Patiala House Court in March 2025 said that the increasing number of cases of possession an exchange of CSEAM, indicates towards the need of strict enforcement mechanism for cyber laws to protect the moral integrity and psychology of children. Accordingly, Anurag Sharma, who was possessing and downloading over 180 files of CSEAM was convicted under Section 67B(b) of the Information Technology Act of 2000. Through its initiative Online Child Sexual Abuse and Exploitation (OCSAE), Central Bureau of Investigation traced his activities through cyber tip-offs and seized all the incriminating digital evidence.

In another case of *State of Uttar Pradesh v. Abid Khan*,[11] the POCSO Special Court of Aligarh, in reference to Section 128 of BNS, 2023, held on 12th February 2025 that online abuse constituted an aggravated form of sexual violence and when the criminal conduct was broadcasted it multiplied the trauma and extended the abuse to a digital audience to an infinite degree. In this notorious case Khan was sentenced to life imprisonment for raping and digitally filming a minor girl and later on distributing the content on an online platform. He was prosecuted under Section 4 and 6 of POCSO Act, Section 67B of IT Act and Section 128 and 95 of Bharatiya Nyaya Sanhita of 2023.

In a similar case of *Central Bureau of*

10 Central Bureau of Investigation v. Anurag Sharma, CBI, Special Court New Delhi, Case No. SC/1324/2017.
11 State of Uttar Pradesh v. Abid Khan, the POCSO Special Court of Aligarh, UP, in Case No. 148/2023.

Investigation v. Rakesh Meena,[12] the CBI Court of Hisar, Haryana, in its judgment dated 30th March 2025 sentenced culprit Meena imprisonment for life. The CBI traced him using Interpol's ICSE (International Child Sexual Exploitation) database and Google's Cyber-Tipline. He was a disabled man, who raped minor boys and uploaded the footage of abuse on the pornographic websites, for which he was charged under Sections 4, 6, 14 and 15 of POCSO along with Section 67(B) of IT Act and Section 128 of Bhatia Nyaya Sanhita.

In the case of *Indore Cyber Cell v. Suresh Patel*, the State Cyber Cell of Indore,[13] sentenced Patel with four years of imprisonment and fine of Rs. 1 Lakh, stating that Digital messaging apps are informal in nature and hence, become a fertile ground for the circulation of the child abuse content and therefore, the law must respond to it with a proportionate force, in a prompt manner. He was a 60 years old man, who shared CSAEM via WhatsApp and tempered the evidence after receiving a police notice. He was convicted under section 67B of IT Act of 2000.

Suggestions

Cyberspace is a necessary evil; as along with being a place that provides education, knowledge, skills, and entertainment, it also creates an environment wherein vulnerabilities are preyed on. Children are the future of a country and hence it is collective social and legal responsibility, of us all, to act proactively to ensure that the well-being of the children is protected and upheld. In order to create a holistic approach; it is important that all the Internet players, law makers, law enforcement agencies, psychologists, and counsellors, collectively understand their responsibility and be part of the mechanism of making cyberspaces safe and children friendly. A few recommendations for the same are enlisted below;

- It Is very important to establish an age-appropriate screen time limit for the children and for that parents and guardians should define A consistent and clear rule about the screen time based on the age of the children. Also, one can use parental control tools and appropriate device settings to enforce these time limits.
- Children must be encouraged to engage in offline activities such as outdoor play, sports or reading for their cognitive development and mental and physical health a structured routine can prevent compulsive digital behaviours from developing and ultimately resulting into digital addictions.
- Secure browsers and age-appropriate apps must be used with effective filters blocking unsafe websites and these controls must be regularly updated from exposing to harmful content.
- A trusting environment should be created where children can feel comfortable discussing their online interactions and experiences with parents needed, guardians or teachers so that early intervention can be ensure before the problem can escalate.
- Accountability for the digital behaviour must be taught to the children at a very young age before exposing them to the digital world so that they are not sharing their personal information, intimate pictures, passwords, etc. online without understanding their repercussions.

12 Central Bureau of Investigation v. Rakesh Meena, the CBI Court of Hisar, Haryana in Case No. 89/2024.
13 Indore Cyber Cell v. Suresh Patel, the State Cyber Cell of Indore in case NO. 67/2025.

- The risk of grooming, making fake profile, etc. should be discussed with children. Their screen usage and social media engagement must also be monitored and supervised by the adults.
- Parents must teach their children especially teenagers about their rights under the laws like POCSO Act, 2012 and IT Act, 2002 etc. which might save them from online abuse and can also make them aware about the reporting mechanism available in the law. Legal awareness also empowers the children to say no and seek timely intervention and help.
- Children must also be encouraged to know, the reporting process of suspicious messages bullying or online threads through National Cyber-Crime Reporting Portal and schools must involve their IT departments in demonstrating this process so that, a digital awareness is created in the children.
- Schools can also host digital-detox drives, and role-play sessions to demonstrate safe online conduct and a community-based approach can also be used to reinforce consistent message across the home and school to ensure safety of children. Cyber laws and Information Technology laws and guidelines can be added to the curriculum of the schools.
- In India, we currently lack a clear legal definition of online grooming. However, POCSO Act and the IT Act covers its elements in digital exploitation. It is important that a dedicated provision along with the law enforcement is created to identify the predatory patterns early.
- It must be made legally binding for the schools to conduct annual digital safety audits as per CBSE or NCERT guidelines related to cyber security and data privacy policies involving children.
- At district level, a dedicated cyber police unit focused upon child protection to handle the complaints of cyber-crime should be established. The officers in these units should specialise in digital forensic child psychology and preservation of evidences and would further facilitate cyber-safety and justice delivery at ground level.
- It is very important to create a stringent and mandatory reporting mechanism to attribute, accountability to all the digital platforms, for which amendment in the Intermediary Guidelines under IT Act is required, to have a visible 'report abuse' or 'flag content' button, a 24/7 redressal mechanism and monthly audit on actions taken against the cyber-crimes, reported. Non-compliance must be taken seriously and financial penalties or suspension of the platform operations in India must be ensured.
- For high-risk apps and games, legally there should be a robust age verification mechanism, supported with government issued ID verification, so that access to mature content, exploitation through addictive games and financial frauds can be prevented.
- The ambit of Digital Personal Data Protection Act of 2023 can be expanded by adding some child-specific clauses; like: prohibition of behavioural tracking and targeted advertising for the users below the age of 18 years, requirement of explicit parental control for processing any personal data of a child and an explicit mandate requiring data anonymity, wherever it is feasible, etc. Law must penalise

any act of violation involving data of a minor which must include blacklisting of repeat offender platforms in India.

- A confidential digital registry for individuals who are convicted of online crimes against children must be maintained and monitored by the court. The access to this digital registry can be given to the police and child welfare agencies for background checks in case involving child cyber abuse this will deter the offenders and will improve due diligence by the institutes.

Conclusion

Establishing a blockchain-secured and AI powered Child Guardian Network (CGN) as an innovation to extend psycho legal framework can help in dealing with cyber delinquencies in children. The CGN can deploy biometrics for analysis of real time sentiments through flagging grooming or bullying using NLP Anomaly Detection. Decentralised ledgers ensuring immediate incident reporting and auto triggering the alerts to the AI-judges, established under POCSO and IT Act can create a stringent enforcement. Using VR-therapy modules can also be used to deliver personalised cognitive rehabilitation blending the Indian support system with coping mechanism for trauma recovery. It is important to adapt a three-dimensional approach and create a holistic mechanism to not only prevent but also to protect the children along with creating a quick and aggressive redressal mechanism in cases digital abuse against children.

Reference

Archard, D., & Macleod, C. B. (2008). Children and the law. Oxford University Press.

Central Board of Secondary Education. (2020). Cyber safety handbook for students. CBSE.

Child Rights International Network. (2018). Children's rights in the digital age. CRIN.

Graber, D. (2017). Raising kids in the digital age: The best apps, websites, and online activities for kids. Mantra Books.

Hinduja, S., & Patchin, J. W. (2016). Cyberbullying and the law: An examination of law and policies. Cyberbullying Research Center.

Lasser, J. (2016). The tech-savvy child: How to protect your kids from the dangers of the digital world. Tarcher Perigee.

Mitchell, K. J., et al. (2009). The impact of Internet use on children's social and psychological development. Pediatrics, 123(6), 1222–1227.

National Council of Educational Research and Training. (2019). Cyber safety and security: A handbook for students. NCERT.

National Council of Educational Research and Training. (2021). Guidelines on digital literacy and cyber safety for schools. NCERT.

Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and suicide: A review of the literature. Archives of Suicide Research, 14(3), 205–217.

Walker, M. L. M. (2018). Understanding the digital generation: A parents' guide to raising kids in the age of technology. Tyndale House Publishers.

Internet Watch Foundation. (2020). Annual report on online sexual abuse and exploitation. IWF.

14. Natural Language Processing (NLP) refers to AI techniques that analyse and interpret human language from text or speech, enabling machines to understand context, sentiment, and intent.