JUVENILE CYBER DELINQUENCY: A STUDY OF TRENDS AND TRIGGERS

Vartika Mishra, Research Scholar, School of Legal Studies, Sangam University, Bhilwara.

Dr. Vishwadeepak Bhatnagar, Emeritus Professor, School of Legal Studies, Sangam University, Bhilwara

ABSTRACT

The rapid growth in digital technology in India poses a twofold challenge: vast potential for "digital natives" and growing threats of cybercrime. This research paper examines the multifaceted drivers and routes into cyber delinquency among Indian juveniles. Based on recent data from the National Crime Records Bureau (NCRB), scholarly works, and case studies, it identifies major psychological, sociological, economic, educational, and technological determinants of these behaviours. The research sheds light on a remarkable increase in cybercrimes against children and stresses the pressing need to view juveniles as both victims and offenders. Though India's legal statutes, in particular the Juvenile Justice (Care and Protection of Children) Act, 2015, set a focus on rehabilitation, the paper lays bare crucial loopholes in existing interventions, such as poor infrastructure, the absence of specialized care, and ongoing societal stigmatization. Based on these findings, this paper suggests a series of evidence-based proposals aimed at holistic digital literacy, rehabilitation ecosystems, legal and enforcement mechanisms, and a victim-centric approach to create a safer digital space for the youth of India.

I. Introduction

India is experiencing a historic digital revolution with more than 800 million internet users and a huge mobile subscriber base of 1.2 billion. One-stop digitization has developed a generation of "digital natives," who are well-versed with technology and well embedded in social structures in the cyber world. Yet, this ubiquitous digital existence creates a paradox: in addition to prospects for acquiring knowledge and bonding, it accords immense vulnerabilities, especially to impressionable youth.[1] The overall incidence of cybercrime in India has shown a consistent upward trend, doubling from 21,796 cases in 2017 to 52,974 in 2021.[2] Recent statistics paint an even grimmer picture, with more than 7,40,000 cybercrime cases reported to the Indian Cyber Crime Coordination Centre (I4C) alone in the first four months of 2024.[3]

Children and teenagers, because of their early and widespread exposure online, faring worse than their proportion of the population, are disproportionately impacted by this trend, finding themselves vulnerable as both victims and, increasingly, as perpetrators of cybercrime. This emphasizes an urgent need to know the dynamics of youth participation in cyber delinquency, going beyond traditional interest in children as victims only. This is a classic example of a large "digital paradox" in the Indian context. The digital platforms and technologies that empower and connect Indian youth at the same time expose them to severe risks, such as harassment, pornography, gambling, and disinformation.[4] The explosive increase in digital access, as a development indicator, has at the same time produced intensified vulnerabilities and new criminal opportunities by and among young people. This built-in contradiction points to an imperative of the moment: it is not feasible or desirable to limit access to the digital space in a tech-reliant society. Instead, focus must be laid on developing secure, responsible, and ethical digital experience, recognizing the double-edged nature of technology in youth life.

---

[1] Sikkim Express, *Escalating Juvenile Delinquency in the Digital World*, https://www.sikkimexpress.com/news-details/escalating-juvenile-delinquency-in-the-digital-world (last visited June 1, 2025).
[2] Ronak Gupta & Neha Dubey, A Study of Cyber Crime Awareness among the Youth, 14 Int'l J. Hum. & Soc. Sci. Invention 97, 97-100 (2025).
[3] Rahul Tripathi, *Indians Lost over ₹1,750 Crore to Cyber Fraud in First Four Months of 2024*, The Economic Times (May 27, 2024), https://economictimes.indiatimes.com/news/india/indians-lost-over-1750-crore-to-cyber-fraud-in-first-four-months-of-2024/articleshow/110444616.cms.
[4] Sikkim Express, supra note [1].

Problem Statement:

The Ever-Rising Problem of Juvenile Cyber Delinquency

The rising involvement of Indian youth in cybercrime is an urgent social problem. Alarming trends have revealed that cybercrimes specifically targeting or involving children have grown many times over, rising fifteen times from 88 cases in 2017 to 1,376 in 2021.[5] The NCRB report for 2022 further confirms the alarming trend, recording a 32% increase in cybercrimes against children from the previous year, reaching a total of 1,823 cases.[6] The increase marks a paradigm shift in the character of crimes among children from such classic crimes as petty theft and vandalism to more sophisticated and technology-based issues such as cyberbullying, digital deception, and other cyber-based crimes unheard of until recently.[7] This emerging phenomenon threatens not only the overall development and well-being of the involved children but also the future security and stability of the nation, calling for urgent and comprehensive attention from policymakers, legal experts, teachers, and families alike.

Research Objectives

- To define juvenile cyber delinquency in India.

- To examine recent trends of juvenile cyber delinquency in India.

- To analyze the factors contributing to the juvenile cybercrime in India.

- To assess the existing legal and rehabilitative frameworks addressing juvenile cyber delinquency in India.

- To recommend strategies aimed at reducing recidivism among juvenile cyber offenders that contribute towards creating a safer and more secure cyberspace for vulnerable youth and the broader community.

---

[5] Satyarthi Global Policy Institute for Children, *Entangled in the Web: Cybercrimes Against Children in India*, 1 (2023).

[6] Mohua Das, *Child Cyber Crime Surges 32% Reveals NCRB Data, Underlining Vulnerability to Online Risks*, The Times of India (Jan. 26, 2024).

[7] DTE Staff, *Over 1,800 Cases of Cybercrimes Against Children Registered in 2022, Higher Than Last Year: NCRB*, Down To Earth (Dec. 6, 2023), https://www.downtoearth.org.in/governance/over-1-800-cases-of-cybercrimes-against-children-registered-in-2022-higher-than-last-year-ncrb-93236.

II. Conceptualizing Juvenile Cyber Delinquency in India

Defining "Juvenile" and "Child" in Indian Law

Legal definitions of "juvenile" and "child" are the building blocks around which the contours of juvenile cyber delinquency in India are determined. The focal legislative statue in this regard is the Juvenile Justice (Care and Protection of Children) Act, 2015 (JJ Act, 2015).[8] The JJ Act, 2015 defines a "juvenile" as a person who is below the age of 18 years. A "child in conflict with law" is defined specifically as a child who is alleged or found to have committed an offense and is below the age of 18 years on the day of committing such offense.[9] This definition is generally in line with the universal standard adopted by the United Nations Convention on the Rights of the Child (UNCRC), which defines a child as every human being below the age of 18 years. The Juvenile Justice (Care and Protection of Children) Act, 2015, is a better version of India's juvenile justice law, supplanting earlier laws passed in 1986 and 2000.[10] One of the most significant reforms made by the 2015 Act is the provision that allows juveniles between the ages of 16 and 17, who are accused of committing "heinous crimes" (offences punishable with imprisonment for seven years or more), to be tried as adults. This key amendment was made in response to public outcry all over the nation after high-profile cases such as the 2012 Delhi gang rape, where the involvement of a juvenile triggered national debate on the adequacy of existing laws.[11] Despite this shift toward the possibility of trying serious criminals as adults, the very philosophy of the Indian juvenile justice system continues to be rooted in the principles of reform and rehabilitation and not purely punitive actions.[12] The emphasis is still on the best interests of the child, with the hope of rehabilitating juvenile offenders into productive citizens through education, vocational training, and psychological counselling. It can be noted that while the JJ Act, the POCSO Act, 2012, and the new Bhartiya Nyaya Sanhita, 2023, use "child" as below 18 years, some of the earlier Indian laws have differential cut-offs in age. For instance, the Child and Adolescent Labour (Prohibition and Regulation) Act (1986/2016) uses "child" as below 14 and "adolescent" as 14-18 years, and the Immoral Traffic (Prevention) Act, 1956,

---

[8] Law Pedia, *Juvenile Justice & Children's Rights*, Times of India Readers' Blog (Jan. 7, 2023), https://timesofindia.indiatimes.com/readersblog/lawpedia/juvenile-justice-childrens-rights-48941/.
[9] Drishti Judiciary. *Difference Between Child and Juvenile.* (Jan. 7, 2025), https://www.drishtijudiciary.com/to-the-point/bharatiya-nyaya-sanhita-&-indian-penal-code/difference-between-child-and-juvenile.
[10] Law Pedia, supra note [8].
[11] Advocate Tanwar, *Juvenile Laws in India: An In-Depth Analysis* (Feb. 5, 2025), https://advocatetanwar.com/juvenile-laws-in-india-an-in-depth-analysis/.
[12] Drishti Judiciary, supra note [9].

uses "child" for below 16 and "minor" for 16-18 years.[13]

This renders the legal situation confusing and possibly inconsistent for determining age-suitable reaction and culpability in various types of offenses. This case represents a "blurring of lines" in juvenile cyber responsibility. The legal system attempts to balance the inherent vulnerability of the child with the necessity of accountability, aiming at older adolescents who commit serious offenses. But the variable definitions of "child" included in different statutes, combined with a significant lack of awareness on the part of juveniles regarding the legal consequences of their online activity, presents a challenging dilemma. Most youth play out activities like digital piracy or forward inappropriate material without realizing that these "trivial"-appearing online activities entail deep legal repercussions.[14] This commentary suggests that interventions must not only emphasize deterrence of serious crime but also general, age-specific education that outlines the legal and ethical bounds of online behaviour, given that developmental stages may interfere with a full conception of consequences.

The categorization of cybercrimes relevant to juveniles

Cybercrime, by definition, defies a single, general definition. Nevertheless, it generally involves any illegal activity that is committed on or via computers, the internet, or other computer-based technologies offensive to human sensibilities.[15] Offenses can be broadly categorized based on their immediate target:

A. Cybercrimes against persons: include a wide range of crimes that have direct victimization of persons, often juveniles who serve as both victims and offenders.

- **Child Pornography, or Child Sexual Abuse Material (CSAM)**: It has been labelled as a most abhorrent cybercrime. It involves the production, transmission, distribution, posting, and publication of sexually explicit material depicting children. Its use witnessed a disheartening 95% rise during the countrywide COVID-19 lockdown, which indicates a heightened vulnerability during periods of greater online

---

[13] Drishti Judiciary, supra note[9].
[14] Astha Srivastava & Shivangi Sinha, Cyber Delinquency: Issues and Challenges Under Indian Legal System, 8 Int'l J. Eng'g & Advanced Tech. 1426, 1426-28 (2019), https://doi.org/10.35940/ijeat.E1204.0585C19.
[15] *A Handbook for Adolescents/Students on Cyber Safety*, Ministry of Home Affairs, Government of India (Dec. 3, 2018).

consumption.[16]

- **Cyberbullying and cyberstalking:** It involve systematic harassment, impersonation, and social ostracism carried out through electronic media.[17] It is interesting to observe that cyberbullying is a serious issue now, with over 33% of Indian children claiming to have been bullied.[18]

- **Cyber Harassment** includes all types of harassment—sexual, racial, religious, or otherwise—happening in cyberspace, which is generally a serious offense against the privacy of the victims.[19]

- **Sextortion and online grooming** are subtle crimes that include forcing, tricking, or manipulating people, especially children, into sex or taking advantage of them through fake online friendships. Cyber groomers use online gaming forums, chat rooms, and fake profiles to build trust with their targets before exploiting their vulnerabilities later.[20]

- **Identity theft** entails the illegal use of another's identification information with the aim of perpetrating fraud, opening bank accounts, or engaging in any other illegal activities.[21]

- **Cyber Suicides** is a new and sad type that refers to cases where suicide was enabled or even broadcast live using technology, thus emphasizing the extreme negative potential of online-based media.[22]

B. Cybercrimes against property are primarily aimed at digital property, systems, and

---

[16] *Satyarthi Global Policy Institute for Children*, supra note [5].

[17] A *Handbook for Adolescents/Students on Cyber Safety, supra note* [15].

[18] Vijayarani M., Balamurugan G., Sevak S., Gurung K., Bhuvaneswari G., Sangeetha X., Thenmozhi P., & Tamilselvi S., *Silent Screams: A Narrative Review of Cyberbullying Among Indian Adolescents*, 16(8) Cureus e66292 (2024).

[19] *Cyber Crime – FAQs*, Education – Vikaspedia, https://education.vikaspedia.in/viewcontent/education/digital-litercy/information-security/cyber-crime-faqs?lgn=en (last visited May 31, 2025).

[20] Jaya Thapa, *The Protection of Children from Cyber Crimes in India*, 6 Int'l J. Multidisciplinary Research 1 (May–June 2024).

[21] Retaj Nadeem & Sadaf Rehman, *E-Vulnerability: How Cybercrimes Are Entangling Youth As Both Victims and Perpetrators*, Virtuosity Legal (Apr. 30, 2025), https://virtuositylegal.com/e-vulnerability-how-cybercrimes-are-entangling-youth-as-both-victims-and-perpetrators/.

[22] Srivastava & Sinha, supra note [14].

information.

- **Illegal Computer Trespass, Vandalism, and Damaging Programs** encompasses unauthorized access to computers, knowingly destroying them, or generating and spreading harmful software such as viruses that inflict irrevocable damage.[23]

- **Hacking** is the process of illegally gaining entry into another person's computer, online account, or device in order to steal information or cause chaos.[24]

- **Software piracy and internet piracy** are the sale of illegal and unauthorized copies of computer programs, movies, or recordings. Teenagers typically do this unknowingly that it is illegal.[25]

- **Online Fraud** involves fraud schemes that are designed to trick people into sending money or releasing personal information. This broad category ranges from phishing attacks to steal sensitive information[26] to money laundering and sophisticated "digital arrest" scams where scammers pose as law enforcement officers to threaten victims into sending money.[27]

C. Other Categories:

Drug Trafficking internet may also serve as a means for the buying and selling of illegal drugs, hence involving adolescents in distribution channels.[28]

Cyberbegging is the new problem involving the exploitation of children through internet means for begging purposes, a specific problem that has been determined not to be dealt with directly by the existing IT Act, 2000, and hence a legislative gap.[29]

Sharenting involves parents posting too much personal information about their kids on the internet, without realizing the long-term implications of the same on their kids' privacy and

---

[23] *Cyber Crime - FAQs - Education*, supra note [19].
[24] Nadeem & Rehman, supra note[21].
[25] Cyber Delinquency, supra[14].
[26] A Study of Cyber Crime Awareness, supra[2].
[27] Delhi Police Arrests Four Men for Rs 44.50 Lakh "Digital Arrest" Fraud, *The Indian Express* (May 31, 2025).
[28] Srivastava & Sinha, supra note[14].
[29] Satyam Mangal, *Safeguarding Digital Childhood: A Critical Analysis of the IT Act, 2000 in Addressing Cyberbegging and Sharenting*, 6 J. Rts. Child NLUO 131, 131-42 (2025).

security.[30]

III. Trends and Statistics on Juvenile Cybercrime in India

The Indian Cybercrime (2017-2025)

The Indian digital revolution has been accompanied by a substantial and steady increase in the number of cybercrime cases. National records indicate that the number of reported cybercrime cases nearly doubled from 21,796 in 2017 to 52,974 in 2021.[31] In 2022, the National Crime Records Bureau (NCRB) recorded 50,035 cases.[32] This pattern has continued unabated, with newer statistics up to April 2025 showing a 24.4% increase in cybercrime, resulting in the registration of over 65,000 First Information Reports (FIRs).[33]

State/UT-wise cases registered under cyber-crimes over the past three years in India (2020-2022)

According to the data published by the National Crime Records Bureau (NCRB) in its *Crime in India* report (2022), the following graph represents the State/UT-wise cases registered under cyber-crimes over the past three years.[34] (Fig 1)

---

[30] Mangal, supra note[29].

[31] *Satyarthi Global Policy Institute for Children, supra note* [5].

[32] Bhavana Sharma & Gaurav Kataria, *Internet Ubiquity and Cybercrime Targeting Children in India*, 6 J. Positive Sch. Psychol. 5103, 5103-12 (2022).

[33] TheCSRUniverse Team, WHT NOW NGO Launches Program To Tackle Rising Cybercrime In India, THE CSR UNIVERSE (Apr. 20, 2025), https://thecsruniverse.com/articles/wht-now-ngo-launches-program-to-tackle-rising-cybercrime-in-india.

[34] Press Information Bureau, Govt. of India, *Increase in Cyber Crimes*, Ministry of Home Affairs (Feb. 7, 2024), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505.
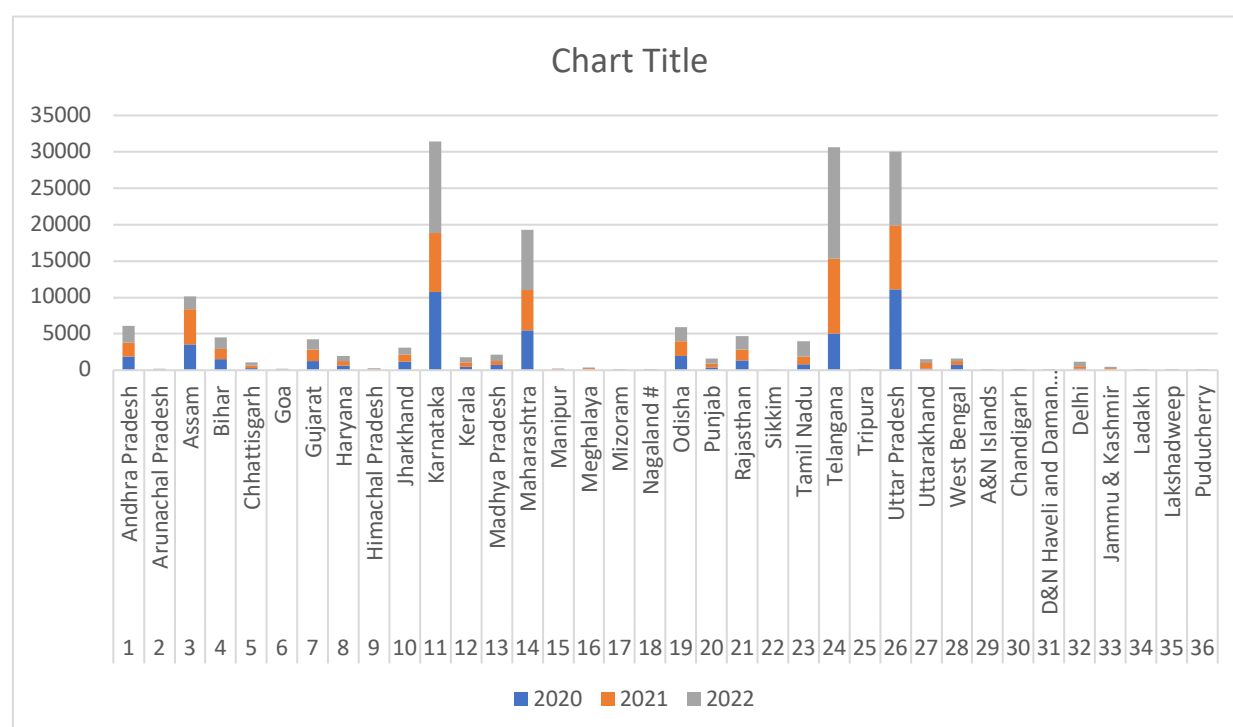
Fig 1: State/UT-wise cases registered under cyber-crimes over the past three years in India (2020-2022)

Experts, however, opine widely that the actual number is far greater, considering that a large proportion of victims, including women and children, are reluctant to report cases either out of fear, social stigma, or lack of knowledge about reporting procedures.[35] The Indian Cyber Crime Coordination Centre (I4C) also registered over 7,40,000 cybercrime cases for the first four months of 2024 alone, with nearly 85% of complaints relating to online financial scams.[36] One of the principal forces driving this boom was the COVID-19 pandemic. The lockdown-imposed forced shift to online learning and greater use of digital media for entertainment and communication in confinement by default inadvertently put children at increased risk and vulnerability. During this time, there was a shocking increase in children's online exposure, often without the presence of adults, thus rendering them fertile ground for their victimization as well as, in some cases, their active participation in perpetrating cybercrimes. For example, the viewing of child pornography surged by a whopping 95% during the lockdown across the country.[37]

---

[35] Mohua Das, *supra* note [6].

[36] Bilal Ahmad, Bilal Ahmad Mir & Sameer Wani, *The Dark Side of Connectivity: Examining the Role of Social Media in Rising Crime Rates in India*, 3 History 30 (2025), https://doi.org/10.5281/zenodo.14907248.

[37] *Satyarthi Global Policy Institute for Children, supra* note [5].

This speaks to how the pandemic served as a powerful accelerant, thrusting many children into the digital space without adequate preparation and protection. This "COVID-19 digital acceleration" highlights the imperative and ongoing necessity for scalable digital literacy and safety education programs among children, their parents, and educators. The shift to online spaces for education, socialization, and entertainment is one that is long-term and requires a proactive, ongoing, and adaptive response to cyber safety protocols, in light of the deep and lasting imprint of this acceleration.

Individual Trends in Cybercrimes against Children

Cybercrimes against or involving children have recorded a shocking and exponential increase. Between the period 2017-2021, reported cases rose fifteen times, from 88 to 1,376. The NCRB 2022 report recorded 1,823 cases of cybercrimes against children, a staggering 32% increase from that of 1,376 in 2021.[38] (Fig 2)
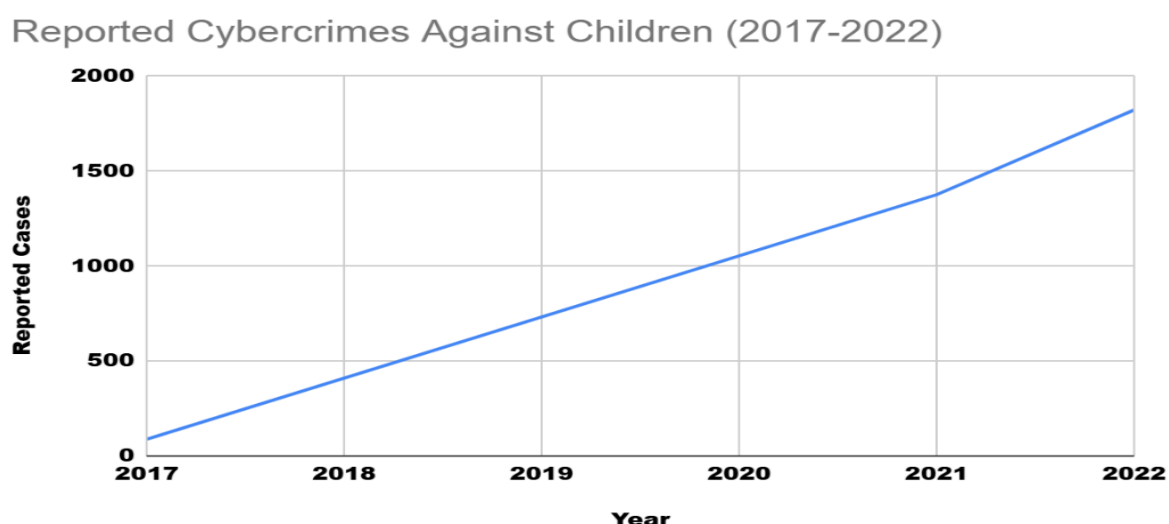

Fig 2: Reported cyber-crimes against Children (2017-2022)

An examination of the cases in 2022 establishes the main forms of cybercrime targeting children: 1,171 were cases of cyber pornography or transmission of inappropriate content, 158 cases were related to cyberstalking and bullying and 416 were part of other cyber child-related crimes.[39] Sexual exploitation was recognized as the second-most common reason for the incidence of cybercrimes in general in the year 2021, and it accounted for 8.6% of the overall incidents of cybercrimes. It was seen that close to 90% of cybercrimes against children in 2020

---

[38] *Satyarthi Global Policy Institute for Children, supra note* [5].
[39] Mohua Das, *supra* note[6].

consisted of dissemination or transmission of Child Sexual Abuse Material (CSAM). The percentage of cases registered under Section 67B of the Information Technology Act (IT Act), which is specifically related to cybercrime against children, indicated a five-fold rise from 3% in 2017 to 15% in 2021. Cases of cyberstalking (according to IPC Section 345D) also indicated a sharp rise, from 7 in 2017 to 123 in 2021.[40] Apart from that, cyberbullying has also become a fast-growing concern with over 33% of Indian children indicating that they have been cyberbullying victims.[41] The figures reported, while undoubtedly worrisome, probably reflect only a percentage of the actual cases of cybercrimes against children. This indicates a "hidden epidemic" of underreported cybercrime. While the rise in reported cases can be partly explained by increased awareness resulting in increased FIR registrations, experts warn that many cases, especially in rural pockets, probably remain unreported.[42]

Additionally, a key hindrance to reporting is hesitation on the part of victims, particularly women and children, out of fear, social stigma, or ignorance about reporting procedures.[43] This observation points out that the actual extent of the problem is probably much larger than official numbers reflect, calling for more widespread resource deployment and community sensitization. Rehabilitative and prevention efforts must not only target the reported cases but also aim at developing safer reporting environments, diminishing the widespread stigma surrounding victimization, and raising awareness to motivate more victims and their families to report.

Geographical Distribution and Age Structure of Victims and Perpetrators.

Although available information is vast, it reflects a lack of detailed information particularly on juvenile cybercrime offenders. Generally speaking, typical cybercrime offender profiles are found to be in the age range of 18 to 30 years and then 30 to 45 years.[44] It is, however, observed that individuals in the age range of 15 to 24 years are "most involved in cyber-crime as well as victims of cyber-crime.[45] The provision in the JJ Act, 2015, for trying older juveniles (16-18) as adults for serious offenses acknowledges implicitly their increasing participation in serious

---

[40] *Satyarthi Global Policy Institute for Children, supra note*[5].
[41] Vijayarani et al., *supra* note[18].
[42] Mohua Das, *supra* note[6].
[43] TheCSRUniverse Team, supra note[33].
[44] P. Kumar, *Growing Cyber Crimes in India: A Survey*, in Proc. 2016 Int'l Conf. on Smart Appl. & Innovative Comput. (SAPIENCE) 246 (2016), https://doi.org/10.1109/SAPIENCE.2016.7684146.
[45] Anam & Shailesh Sharma, *A Study on Indian Youth and Cyber Crime*, 4 Career Point Int'l J. Rsch. 67 (2022).

offenses. It has recently surfaced through a case that juveniles of 13 and 14 years were arrested for mobile snatching and high-tech cyber fraud, thereby indicating the participation of even younger individuals in organized crime groups.[46] Children have been reported to be most susceptible to cybercrime, with an overwhelming 32% of parents confirming negative experience for their children on the internet, ranging from cyberbullying, impersonation, and child pornography exposure.[47]   There is a broad gender disparity when it comes to victimization: close to 99% of sexual crime victims among children and 97% of POCSO cases are girls, and the culprits are those close to the victims.[48]

The geography of child crimes and cybercrimes indicates clear concentrations.

- Five states accounted for close to half of all crimes against children during 2022: Maharashtra (12.8%), Madhya Pradesh (12.6%), Uttar Pradesh (11.5%), Rajasthan (5.8%), and West Bengal (5.5%).[49] (Fig 3)

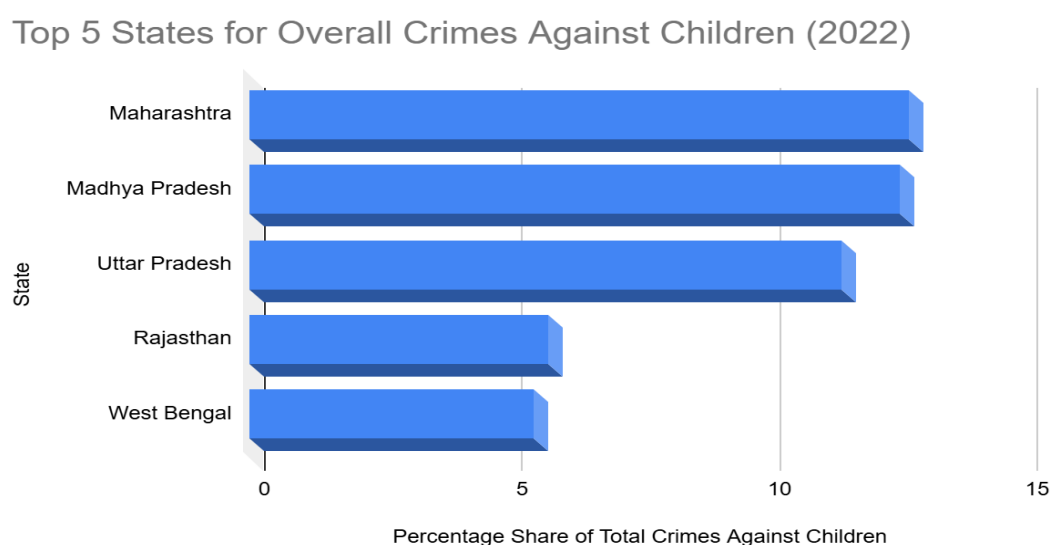Top 5 States for Overall Crimes Against Children (2022)

Fig 3: Top 5 States for Overall Crimes Against Children (2022)

- For child cybercrimes in 2022, Madhya Pradesh had 147 cases (third highest in the

---

[46] HT Correspondent, *4 Gang Members, 3 Minors Arrested for Mobile Theft, Cyber Fraud*, Hindustan Times (Apr. 20, 2025), https://www.hindustantimes.com/cities/lucknow-news/4-gang-members-3-minors-arrested-for-mobile-theft-cyber-fraud-101745168423203.html.
[47] Ministry of Home Affairs, *supra* note[15].
[48] Mohua Das, *supra* note[6].
[49] DTE Staff, *supra* note[7].

country), trailed by Karnataka with 239 cases and Rajasthan with 161.44.[50]

- The overall rate of cybercrime during 2021 was the highest in Karnataka (16.2%), followed by Telangana (13.4%) and Assam (10.1%).[51]

- A disturbing trend has been observed, and it indicates that youth from southern Indian states like Tamil Nadu (leaving out Kerala) and northern states like Uttar Pradesh, Rajasthan, and Bihar are being attracted in growing numbers to Southeast Asian countries for lucrative offers. This group of youth is most susceptible to being cheated by fake online job advertisements for high-paying technological jobs, and this can result in their trafficking into global cyber scam networks, thus becoming unwilling actors in organized cybercrime activities.[52]

IV. Motivations and Routes to Cyber Delinquency among Indian Juveniles

A complete understanding of the drives and directions that lead Indian youth into cyber delinquency involves an all-around analysis that encompasses socio-psychological, socio-economic, educational, and technological factors along with the exploitative mechanism's underneath.

A. Socio-Psychological Factors

- **Cyber Unawareness and Digital Illiteracy:** The widespread and serious cause of juvenile cyber offending is the profound lack of proper knowledge among youths regarding online security, privacy controls, and protective measures.[53] It is not just that they become easy prey to cybercriminals but also unknowingly guide many to commit offenses without realizing the complete legal consequences. Common examples include digital piracy, such as downloading pirated movies or songs from untrustworthy sites.

- **Peer Influence and Social Media Dynamics:** Adolescents are extremely vulnerable to peer pressure, an influence hugely compounded by the prevalent usage of social media

---

[50] Amarjeet Singh, *Acute Rise in Cyber Crimes Against Kids in Past 5 Years*, Times of India (Feb. 12, 2024).
[51] Sharma & Kataria, supra note[32].
[52] Sreeparna Banerjee, *Cyber Scams and Trafficking: India's Southeast Asian Challenge*, Observer Research Foundation (July 27, 2023), https://www.orfonline.org/expert-speak/cyber-scams-and-trafficking-india-s-southeast-asian-challenge.
[53] Gupta & Dubey, *supra* note[2].

platforms.[54] Being exposed to risk-taking online content, such as the glorification of violence, illegal drug use, or online bullying, can invoke imitation or direct participation in deviant acts, both online and offline. The feeling of anonymity in certain social media platforms, especially those that have vanishing message features such as Snapchat, Instagram, and Telegram, encourages impulsiveness and fatal non-accountability among adolescents. Such anonymity enables them to behave in a manner they would never attempt in face-to-face interactions.[55]

- **Family Environment and Parental Supervision:** A dysfunctional family environment, with neglectful parenting, physical or emotional maltreatment incidents, or a chronic absence of adequate supervision, significantly increases a juvenile's likelihood of engaging in delinquent behaviour. Divorce, chronic conflict in the family, or the absence of consistent parental supervision can trigger behavioural problems and a search for acceptance or approval outside the family, and at times this leads them down the wrong track.[56] One of the main problems is that many parents lack a good understanding of online environments and, therefore, fail to monitor their children's online activity properly.

- **Psychological Factors:** Underlying psychiatric disorders, including depression, anxiety, and conduct disorders, can play a major role in delinquency among juveniles. Cyber-victimization itself can trigger or worsen these psychiatric disorders, resulting in heightened stress, anxiety, and depression. Some juveniles exhibit inherent aggressive tendencies and impulsivity, which, combined with their still-developing cognitive abilities, make them more susceptible to acting out in aggressive or inappropriate ways online.[19]

B. Socioeconomic and Education Factors

Poverty, Unemployment, and the Search for Quick Monetary Reward: Juveniles belonging to economically disadvantaged sections of society, who often lack adequate access to quality education and real career opportunities, are most vulnerable to being lured into illegal

---

[54] Juris Centre, *The Dark Side of the Like Button: Implications of Social Media in Juvenile Delinquency Cases*, Juris Centre (Mar. 15, 2024), https://juriscentre.com/2024/03/15/the-dark-side-of-the-like-button-implications-of-social-media-in-juvenile-delinquency-cases/.

[55] Sikkim Express, *supra* note[1].

[56] Juris Centre, *supra* note[54].

activity. Financial crisis and the ubiquitous problem of unemployment can have the capacity to foster rooted frustration and hopelessness, driving such youths to illegal activity as perceived means of survival or to gain quick monetary reward.[57] Although monetary reward may not always turn out to be the sole or exclusive motive behind every juvenile cybercrime, it is a major factor, with one study indicating that 30% of juvenile offenders perceived it as the main reason behind such crimes.[58]

Educational Issues and School Culture: The education system of India has a serious set of issues that lead to delinquency among the youth. Poor performance in school, disengagement from school, and victimization through bullying or an offending school environment can result in offending behaviour and a crime-prone orientation.[59] In effect, the lack of rigorous cybersecurity education within mainstream education systems is a considerable loophole, leaving young people vulnerable to the sophisticated threats and moral challenges of the digital age.[60]

C. Technological and Exploitative Pathways

- **Ease of Access and Susceptibility to Exploitation:** Extensive availability of low-cost, portable devices with 24/7 internet access is a "genie and the magic lamp" for young people, offering seemingly boundless possibilities for fantasy and exploration for a click.[61] Adolescents are highly susceptible to many covert types of internet exploitation, which are usually enabled by the platforms where they socialize.

- **Grooming:** Cyber groomers intentionally use online game forums, chat rooms, and false personas to try to establish a relationship with teens, thus gaining their trust before exploiting or manipulating them into engaging in sexual activities.[62]

- **Cyberbegging** is a new issue which is connected to the exploitation of children through electronic media for fund-raising, i.e., an issue which is not explicitly covered under

---

[57] Virek Aggrawal, *Rising Juvenile Crime in India: A Crime Against Society? or Crime Stemming in Society*, 11 Indian J. Soc. & Pol. 27, 27–30 (2024).
[58] Gupta & Dubey, *supra* note[2].
[59] ApniLaw, *Understanding Juvenile Delinquency: Causes, Types, and Legal Framework in India*, ApniLaw (Mar. 2025), https://www.apnilaw.com/opinion-analysis/juvenile-delinquency-india/.
[60] TheCSRUniverse Team, supra note[33].
[61] Chhavi Gupta, *Combating the Clutches of Cyber Delinquency in India*, 2 Indian J. Integrated Rsch. L. 1 (2024).
[62] Jaya Thapa, *supra* note[20].

the present IT Act, 2000 and therefore depicts a major legislative deficiency.[63]

- **Internet Trafficking:** Offenders exploit the pervasiveness and anonymity of the internet by using social media, messaging services, and dark web sites to entice, manipulate, and exploit children for illegal labour and sexual exploitation. Some of the new trends in this direction include exploitation of live-streaming and gamified enticement, in which children are groomed using chat platforms and video games.[64]

- **Accidental Offense due to Lack of Knowledge of Legal Sanctions:** An overwhelming majority of juveniles unknowingly commit cybercrime because of an extreme lack of knowledge of the legal sanctions of their cyber activities. Typical examples are online piracy, such as pirated movie or song downloads from questionable websites, or sending abusive emails to schoolmates, without knowing that these are copyright violations or harassment, punishable by severe sanctions.[65]

V. Legal, Policy and Institutional Frameworks for Juvenile Cyber Justice in India

Category	Act/Policy/Body	Key Provisions/Focus	Relevance to Juvenile Cybercrime
Primary Laws	The Juvenile Justice (Care and Protection of Children) Act, 2015	Defines "child in conflict with law" (CICL) as a child alleged or found to have committed an offense who has not completed 18 years of age. Emphasizes rehabilitation and reintegration of children. Categorizes offenses as petty, serious, and heinous. In the case of heinous offenses, juveniles between the ages of 16-18 years can be tried as adults on preliminary examination by the Juvenile Justice Board (JJB).	This is the general law that prescribes how juveniles involved in any crime, such as cybercrime, are treated. It is concerned with the child's welfare, reformation, and rehabilitation.

---

[63] Mangal, supra note [29].

[64] *Cyber Trafficking of Children in India: Emerging Legal Challenges and the Need for Reform*, The Law Way with Lawyers (Mar. 2025), https://thelawwaywithlawyers.com/cyber-trafficking-of-children-in-india-emerging-legal-challenges-and-the-need-for-reform/.

[65] Srivastava & Sinha, *supra* note[14].

	Information Technology (IT) Act, 2000 (and its amendments)	Core legislation for cybercrimes. Sections like 43 (penalties for data theft, hacking), 66 (hacking, identity theft, cyberstalking), 67 (publishing/transmitting obscene material), and 67B (publishing/transmitting child pornography).	Though not technically juvenile, these paragraphs detail some of the computer crimes juveniles can commit. Section 67B is most applicable since it addresses child pornography, which juveniles themselves may be victims of as well as, sometimes, the perpetrators.
	Protection of Children from Sexual Offences (POCSO) Act, 2012	Provides comprehensive protection to children from sexual offenses, including those committed online. Defines "child pornography" (Section 2(da)) and prescribes stringent punishments (Sections 14, 15) for creation, distribution, possession of child pornography.	Directly encompasses online child sexual abuse material (CSAM) that may involve juveniles. It encompasses crimes like online grooming and sexual harassment.
	Bharatiya Nyaya Sanhita, 2023)	Sections like 78 (stalking, including cyberstalking), 356(2) (defamation), 79 (insulting the modesty of a woman).	Some of the provisions of the IPC can be indirectly applied to cybercrimes against or involving juveniles, such as cyberstalking, cyberbullying to the level of defamation or insulting modesty.
Policies & Initiatives	National Cyber Security Policy (NCSP), 2013	Aims to establish a secure and safe cyberspace. Focuses on developing cybersecurity consciousness, public-private cooperation, capacity development, and international collaboration.	Offers a general framework for cybersecurity, impacting awareness campaigns that may educate juveniles of proper

			online conduct and the implications of cybercrime.
	Cybercrime Prevention against Women and Children (CCPWC) Scheme	An integrated central sector scheme under the Ministry of Home Affairs. It is to set up cyber forensic-cum-training labs, equip police organizations, and raise awareness.	Directly addresses cybercrimes against women and children, including juvenile cyber prevention and management by providing awareness and investigation resources and training.
	Indian Cyber Crime Coordination Centre (I4C)	One integrated national platform to deal with cybercrimes in an organized and holistic manner.	Facilitates reporting and investigation of cybercrimes, such as cybercrimes against children.
	National Commission for Protection of Child Rights (NCPCR)	Statutory framework that guarantees policies, programs, and legislation are child rights-oriented.	Coordinates the application of child protection law, for instance, cyber safety, and ensures rights of children in conflict with the law are protected.
Institutional Framework	Juvenile Justice Boards (JJBs)	Established under the JJ Act, 2015, to deal with children in conflict with the law. Conduct preliminary assessments for heinous offenses by juveniles aged 16-18.	The primary judicial body responsible for handling cases of juveniles involved in cybercrime, focusing on their rehabilitation.
	Child Welfare Committees (CWCs)	Deal with children in need of care and protection, including those who may be victims of cyber exploitation.	While not directly working with the juvenile offenders, CWCs are part of the child protection system that is interrelated with cyber safety.

	Cyber Crime Cells/Units in Police Departments	Specialized units within law enforcement agencies for investigating cybercrimes.	Responsible for investigating cybercrime cases, including those where juveniles are involved as perpetrators or victims.
	Cyber Forensic Training Labs	Established to provide forensic analysis capabilities for digital evidence in cybercrime cases.	Essential to evidence collection in juvenile cybercrime investigations, aiding investigations.
Awareness & Education	Cyber Dost (Twitter handle by MHA)	Tweets on cybercrime awareness.	An awareness campaign that educates the public on cybercrimes that can extend to adolescents and parents.
	Handbook for Adolescents/Students on Cyber Safety	Published by the Government to inform about cybercrimes and protection.	A resource specifically designed to educate young people about cyber safety and the risks of cybercrime.
	Guidelines by CBSE on Safe and Secure Use of Internet for Schools	Directs schools to install firewalls, filtering software, and implement security policies.	Aims to make school life more secure on the internet, potentially reducing the scope for juvenile cybercrime.

India's legal code, the Juvenile Justice (Care and Protection of Children) Act, 2015, firmly reflects a progressive inclination in that it places the best interests of the child at the forefront of juvenile justice, with a rehabilitation over punishment approach. Yet even with this robust legal code and progressive ideology, there are deep-seated and complex issues that dilute its aims. These are insufficient infrastructure and provisions in rehabilitation centres, a lack of specialized psychological experts, and the common stigma of juvenile delinquency. This gap

between intention in the law and its practice has implications for the effectiveness of rehabilitative interventions, and it suggests that a robust legal code alone is insufficient without parallel development of infrastructure, training, and societal attitudes.

VI. Conclusion and Recommendations

The digital revolution, though a badge of honour for India's growth, has also brought with it wake a multi-faceted challenge: the new trend of cyber delinquency among young people. The analysis in this paper finds a phenomenal increase in cybercrimes by Indian youth, fuelled by a confluence of socio-psychological vulnerabilities, socio-economic pressures, and the very nature of the digital arena. The "digital paradox" finds that the same technology providing unprecedented opportunities also subjects children to dire perils, which tend to propel them onto a "curiosity-to-criminality" trajectory owing to a severe dearth of digital literacy and awareness of legal repercussions. Additionally, the "parental digital divide" fills in these perils, as parents will likely be deficient in the requisite information to adequately police children's online behaviour.

Although India's legal system, especially the Juvenile Justice (Care and Protection of Children) Act, 2015, is progressive in its approach towards rehabilitation, there is a wide "implementation gap" between legislative vision and reality on the ground. The gap is marked by substandard facilities, lack of resources in the rehabilitation centres, a severe shortage of specialist psychological input, and the ever-present social stigma of juvenile delinquency. Moreover, a "lagging legislation" results in existing legislations being unable to keep up with the swift rate of evolving cybercrime modality and new and emerging threats like online child trafficking find themselves inadequately covered. The issue is further exacerbated by judicial delay and inconsistency in age determination, which can vitiate the very spirit of child-friendly justice.

It is a multi-layered issue that needs to be addressed by a multi-pronged, holistic solution beyond the typical punitive measures. These suggestions are crucial to guide effective rehabilitation programs and encourage responsible digital citizenship among Indian youth:

1. Prioritize Comprehensive Digital Literacy and Cyber Safety Education:

- **Incorporation into Compulsory Curriculum:** Utilize compulsory, age-related cybersecurity awareness modules within school curricula from elementary school

through. These modules should incorporate online security, privacy settings, ethical online behaviour, and the legal consequences of cyber-crimes, including seemingly minor actions.

- **Parental Empowerment Programs:** Create and widely distribute digital literacy and cyber safety programs for parents and custodians. These programs should provide them with the knowledge and tools needed to comprehend online dangers, meaningfully observe their children's cyber activities, and engage in open communication about online activities.

- **Positive Channelling of Curiosity:** Develop and sustain programs that direct juveniles' inherent technological curiosity and aptitude into positive, ethical channels, for example, ethical hacking clubs, coding competitions, and career guidance in cybersecurity.

2. Strengthen Rehabilitation Infrastructure and Programs:

- **Increased Investment:** Make substantial human and financial investment to enhance the observation and special home facilities. This includes ensuring adequate personnel, particularly trained counsellors, psychologists, and vocational trainers, to provide child-centred educational, vocational, and therapeutic services.

- **Individualized Care Plans:** Enforce rigorous use and regular follow-up of Individual Child Care Plans, tailoring interventions to the individual psychological, educational, and social needs of each young person.

- **Community-Based Reintegration:** Set and provide community-based rehabilitation programs that facilitate easy reintegration of the juveniles into the community. These include public information campaigns to minimize stigma and promote community acceptance as well as support systems.

3. Reform Legal and Enforcement Mechanisms:

- **Dynamic Legislative Review:** Provide for periodic legislative review and future amendment of the IT Act, POCSO Act, BNS, and other relevant laws to include new

cybercrimes (e.g., cyberbegging, online trafficking of children) and keep legal definitions and penalties in sync with the evolving digital environment.

- **Specialized Training to Justice Stakeholders:** Provide mandatory and periodic specialized training in cyber forensics, digital investigation, and cybercrime subtleties to prosecutors, judicial officers, and law enforcement agencies. This will enhance their capacity to investigate, adjudicate, and prosecute cybercrime cases involving juveniles effectively.

- **Enhanced Inter-Agency and Cross-Border Coordination:** Enhance the inter-agency cooperation between the national agencies (such as I4C) and the international agencies (such as Interpol) to tackle cross-border cybercrime syndicates and facilitate tracing and prosecution of criminals going across the borders.

4. Promote a Victim-Centred Approach and Support Mechanisms:

- **Accessible Reporting Mechanisms:** Implement and disseminate child-friendly, accessible, and confidential reporting mechanisms (e.g., national hotlines, online reporting websites) for cybercrime victims.

- **Holistic Support Services:** Offer holistic support services, including on-the-spot guidance, legal aid, and extended rehabilitation for child victims, to prevent re-traumatization and promote their healing process.

- **Harness NGO Partnerships:** Work closely with NGOs and civil society actors who have child protection, digital safety, and mental health expertise. These actors typically have good grassroots access and specialist knowledge to enable successful intervention.

By implementing these integrated suggestions, India can take a step towards a strong and sensitive juvenile justice system that responds not only to the immediate challenges of cyber delinquency but also anticipates and provides protection to its children against the snares of the digital era, turning potential criminals into responsible and productive digital citizens.

REFERENCES:

1. *A Handbook for Adolescents/Students on Cyber Safety*, Ministry of Home Affairs, Government of India (Dec. 3, 2018).

2. Advocate Tanwar, *Juvenile Laws in India: An In-Depth Analysis* (Feb. 5, 2025), https://advocatetanwar.com/juvenile-laws-in-india-an-in-depth-analysis/.

3. Amarjeet Singh, *Acute Rise in Cyber Crimes Against Kids in Past 5 Years*, Times of India (Feb. 12, 2024).

4. Anam & Shailesh Sharma, *A Study on Indian Youth and Cyber Crime*, 4 Career Point Int'l J. Rsch. 67 (2022).

5. Anil Rachamalla et al., *Cyber Crime Against Women and Children: It Happens Everywhere: At Home, at Work, at Study, on the Street, in Public Transport and Online Too* (Kindle ed. 2023).

6. ApniLaw, *Understanding Juvenile Delinquency: Causes, Types, and Legal Framework in India*, ApniLaw (Mar. 2025), https://www.apnilaw.com/opinion-analysis/juvenile-delinquency-india/.

7. Astha Srivastava & Shivangi Sinha, Cyber Delinquency: Issues and Challenges Under Indian Legal System, 8 Int'l J. Eng'g & Advanced Tech. 1426, 1426-28 (2019).

8. Bhavana Sharma & Gaurav Kataria, *Internet Ubiquity and Cybercrime Targeting Children in India*, 6 J. Positive Sch. Psychol. 5103, 5103-12 (2022).

9. Bilal Ahmad, Bilal Ahmad Mir & Sameer Wani, *The Dark Side of Connectivity: Examining the Role of Social Media in Rising Crime Rates in India*, 3 History 30 (2025), https://doi.org/10.5281/zenodo.14907248.

10. Chhavi Gupta, *Combating the Clutches of Cyber Delinquency in India*, 2 Indian J. Integrated Rsch. L. 1 (2024).

11. *Cyber Crime – FAQs, Education – Vikaspedia*, https://education.vikaspedia.in/viewcontent/education/digital-litercy/information-

security/cyber-crime-faqs?lgn=en (last visited May 31, 2025).

12. *Cyber Trafficking of Children in India: Emerging Legal Challenges and the Need for Reform*, The Law Way with Lawyers (Mar. 2025), https://thelawwaywithlawyers.com/cyber-trafficking-of-children-in-india-emerging-legal-challenges-and-the-need-for-reform/.

13. *Delhi Police Arrests Four Men for Rs 44.50 Lakh "Digital Arrest" Fraud*, The Indian Express (May 31, 2025).

14. Drishti Judiciary. *Difference Between Child and Juvenile.* (Jan. 7, 2025), https://www.drishtijudiciary.com/to-the-point/bharatiya-nyaya-sanhita-&-indian-penal-code/difference-between-child-and-juvenile.

15. DTE Staff, *Over 1,800 Cases of Cybercrimes Against Children Registered in 2022, Higher Than Last Year: NCRB*, Down To Earth (Dec. 6, 2023), https://www.downtoearth.org.in/governance/over-1-800-cases-of-cybercrimes-against-children-registered-in-2022-higher-than-last-year-ncrb-93236.

16. HT Correspondent, *4 Gang Members, 3 Minors Arrested for Mobile Theft, Cyber Fraud*, Hindustan Times (Apr. 20, 2025), https://www.hindustantimes.com/cities/lucknow-news/4-gang-members-3-minors-arrested-for-mobile-theft-cyber-fraud-101745168423203.html.

17. Jaya Thapa, *The Protection of Children from Cyber Crimes in India*, 6 Int'l J. Multidisciplinary Research 1 (May–June 2024).

18. Juris Centre, *The Dark Side of the Like Button: Implications of Social Media in Juvenile Delinquency Cases*, Juris Centre (Mar. 15, 2024), https://juriscentre.com/2024/03/15/the-dark-side-of-the-like-button-implications-of-social-media-in-juvenile-delinquency-cases/.

19. Karnika Seth, *Computers, Internet and New Technology Laws: A Comprehensive Reference Work with Special Focus on Developments in India* (LexisNexis India 2022).

20. Karnika Seth, *Protection of Children on Internet* (LexisNexis India 2020).

21. *Law Pedia, Juvenile Justice & Children's Rights*, Times of India Readers' Blog (Jan. 7, 2023), https://timesofindia.indiatimes.com/readersblog/lawpedia/juvenile-justice-childrens-rights-48941/.

22. Malik, *DLH's Law of Juvenile Justice in India* (3d ed. 2023).

23. Mohua Das, *Child Cyber Crime Surges 32% Reveals NCRB Data, Underlining Vulnerability to Online Risks*, The Times of India (Jan. 26, 2024).

24. National Crime Records Bureau, Ministry of Home Affairs, Govt. of India, *Crime in India – 2022*.

25. P. Kumar, *Growing Cyber Crimes in India: A Survey*, in Proc. 2016 Int'l Conf. on Smart Appl. & Innovative Comput. (SAPIENCE) 246 (2016), https://doi.org/10.1109/SAPIENCE.2016.7684146.

26. Pavan Duggal, *Cyber Law* (LexisNexis, 2023).

27. Pavan Duggal, *Textbook on Cyber Law* (2d ed. 2016).

28. Press Information Bureau, Govt. of India, *Increase in Cyber Crimes*, Ministry of Home Affairs (Feb. 7, 2024), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505.

29. Rahul Tripathi, *Indians Lost over ₹1,750 Crore to Cyber Fraud in First Four Months of 2024*, The Economic Times (May 27, 2024), https://economictimes.indiatimes.com/news/india/indians-lost-over-1750-crore-to-cyber-fraud-in-first-four-months-of-2024/articleshow/110444616.cms.

30. Retaj Nadeem & Sadaf Rehman, *E-Vulnerability: How Cybercrimes Are Entangling Youth As Both Victims and Perpetrators*, Virtuosity Legal (Apr. 30, 2025), https://virtuositylegal.com/e-vulnerability-how-cybercrimes-are-entangling-youth-as-both-victims-and-perpetrators/.

31. Ronak Gupta & Neha Dubey, A Study of Cyber Crime Awareness among the Youth, 14 Int'l J. Hum. & Soc. Sci. Invention 97, 97-100 (2025).

32. Satyam Mangal, *Safeguarding Digital Childhood: A Critical Analysis of the IT Act, 2000 in Addressing Cyberbegging and Sharenting*, 6 J. Rts. Child NLUO 131, 131-42 (2025).

33. Satyarthi Global Policy Institute for Children, *Entangled in the Web: Cybercrimes Against Children in India*, 1 (2023).

34. Sikkim Express, *Escalating Juvenile Delinquency in the Digital World*, https://www.sikkimexpress.com/news-details/escalating-juvenile-delinquency-in-the-digital-world (last visited June 1, 2025).

35. Sreeparna Banerjee, *Cyber Scams and Trafficking: India's Southeast Asian Challenge*, Observer Research Foundation (July 27, 2023), https://www.orfonline.org/expert-speak/cyber-scams-and-trafficking-india-s-southeast-asian-challenge.

36. The Bhartiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India).

37. The Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).

38. The Juvenile Justice (Care and Protection of Children) Act, No. 2 of 2016, Acts of Parliament, 2015 (India).

39. The Protection of Children from Sexual Offences Act, No. 32 of 2012, Acts of Parliament, 2012 (India).

40. TheCSRUniverse Team, *WHT NOW NGO Launches Program To Tackle Rising Cybercrime In India*, THE CSR UNIVERSE (Apr. 20, 2025), https://thecsruniverse.com/articles/wht-now-ngo-launches-program-to-tackle-rising-cybercrime-in-india.

41. Ved Kumari, *Juvenile Justice System in India: From Welfare to Rights* (Oxford Univ. Press 2017).

42. Ved Kumari, *The Juvenile Justice (Care and Protection of Children) Act, 2015: Critical Analyses* (2d ed., LexisNexis India 2024).

43. Vijayarani M., Balamurugan G., Sevak S., Gurung K., Bhuvaneswari G., Sangeetha X.,

Thenmozhi P., & Tamilselvi S., *Silent Screams: A Narrative Review of Cyberbullying Among Indian Adolescents*, 16(8) Cureus e66292 (2024).

44. Virek Aggrawal, *Rising Juvenile Crime in India: A Crime Against Society? or Crime Stemming in Society*, 11 Indian J. Soc. & Pol. 27, 27–30 (2024).

45. Yatindra Singh, *Cyber Laws* (Universal Law Pub. Co. 2016).