

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 8 | Issue 2

2026

© 2026 International Journal of Legal Science and Innovation

Follow this and additional works at: <https://www.ijlsi.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in the International Journal of Legal Science and Innovation after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Legal Science and Innovation, kindly email your Manuscript to submission@ijlsi.com.

Rethinking Juvenile Justice for the Digital Age: Legal Challenges of Child Cyber-Delinquency in India

LAKSHMI TALUKDAR*

ABSTRACT

Rapid digitisation has opened the way to a range of crimes, including crimes committed by children, giving rise to a new form of juvenile delinquency. Child cyber delinquency has escalated ethical, legal and procedural problems and become a troubling trend in the digital age. Although India's principal child-centric justice framework, the Juvenile Justice Act, 2015, has been modernised over the years and has brought about significant changes, it still fails to address the complexities of cyber delinquency adequately. Acts such as identity theft, phishing, online fraud, hacking and digital extortion not only highlight the growing involvement of juveniles in cybercrime but also underline the need to view children as both offenders and victims. This study uses doctrinal methods to assess the lack of cyber-specific classification, assessment and rehabilitation. The paper critically examines official crime data and police reports, and provides a comparative analysis of selected international juvenile justice models in the United Kingdom, Singapore and New Zealand. It sheds light on the inconsistent treatment of juvenile offenders and on the lack of cyber-psychology and digital maturity assessment. The primary objective is to examine the legal gaps in the principal Act and the legal and moral dilemmas surrounding it, and to propose digital-age reforms for better governance. The paper finds that the current principal legislation reflects a pre-digital mindset, yielding irregular implementation of the law and insufficient rehabilitative outcomes. It argues that the current approach undermines accountability, and it emphasises the urgent need for reforms that integrate cyber-forensic expertise and promote rehabilitation programmes within the juvenile justice framework. The study concludes by proposing targeted policy reforms to strengthen India's child protection legislation while upholding its restorative and rights-based character in the evolving digital ecosystem.

Keywords: *Child Cyber Delinquency, Juvenile Justice Act, Digital Crimes, Cyber Psychology, Juvenile Rehabilitation, Digital Age Reforms*

* Author is a Student at Bennett University, Greater Noida, Uttar Pradesh, India.

I. INTRODUCTION

A. Background of the study

India has been evolving steadily, with a constant focus on digitisation and modernisation. With a massive internet user base, India is on the verge of crossing 900 million internet users, driven largely by growth in rural India.¹ Young Indians are highly engaged online, and many pursue content creation and social media influence. But despite the career opportunities and other merits of the internet, it has become a tool for the proliferation of crimes ranging from bullying and stalking to identity theft and pornography.² A digital dilemma is emerging among the current generation: even though digital platforms are promoted for productivity, creativity, education and career development, the simultaneous use of these platforms for delinquent activities has increased significantly. Children today engage in various internet activities at an early age without adult supervision. This creates a gap marked by the absence of parental awareness, regulatory frameworks and legal consequences, and because of this gap children engage in cybercrimes without understanding the nuances of cyber law. A 2022 McAfee study of Indian families found that 22 per cent of Indian children had experienced cyberbullying, against a global average of 17 per cent, and that many parents lacked the technical skills and understanding needed to keep their children safe online.³ Children are now termed digital natives, known for their fluency with cyberspace, but they often overlook the fact that their limited understanding of consent, privacy and the permanence of online action can lead to dangerous repercussions. High digital fluency without legal awareness paves the way for cyberbullying, hacking, identity misuse and online harassment. Because of this digital paradox, in which rapid digitisation coexists with widening inequalities and limitations, digital exposure may lead to toxic online communities, radicalisation, gambling-like gaming mechanisms and anonymity-driven misconduct.

As the term is used in the literature, delinquency extends to any adolescent conduct that breaches social norms or the law, whether a minor behavioural problem or a serious antisocial

¹ INTERNET & MOBILE ASS'N OF INDIA & KANTAR, *INTERNET IN INDIA 2024 (2025), as reported in India's Internet Revolution: Key Insights from Kantar and IAMAI Report*, BUSINESS TODAY (Jan. 16, 2025), <https://www.bustoday.in/technology/news/story/indias-internet-revolution-key-insights-from-kantar-and-iamai-report-461043-2025-01-16>.

² See Sravani Sarkar, *Cybercrimes Against Children Records 32 pc Increase in 2022: NCRB Data*, THE WEEK (Dec. 6, 2023), <https://www.theweek.in/news/india/2023/12/06/cybercrimes-against-children-records-32-pc-increase-in-2022-ncrb-data.html>.

³ MCAFEE, *LIFE BEHIND THE SCREENS OF PARENTS, TWEENS, AND TEENS: THE 2022 MCAFEE CONNECTED FAMILY STUDY, INDIA (2022), as reported in McAfee 2022 Study Finds Indian Children to Be More Vulnerable Online*, DIGITAL WATCH OBSERVATORY (May 13, 2022), <https://dig.watch/updates/mcafee-2022-study-finds-indian-children-to-be-more-vulnerable-online>.

or criminal act.⁴ Adolescence is a significant transitional stage in human life, which increases a child's vulnerability and makes them prone to stress. The problems they face during this stage, the transformations within themselves and their environment, and their ability to handle such situations all affect their mental health, positively or negatively, and may pave the way for addictive habits. As Yoo observes, features peculiar to cyberspace, among them anonymity, ease of access and the difficulty of monitoring and sanctioning online conduct, leave adolescents especially prone to cyber delinquency. These features lead them to believe that their actions are temporary, untraceable and consequence-free, and therefore free of accountability.

B. Research problem

India's juvenile justice framework was conceptualised at a time when delinquency was largely understood as physical or offline misconduct. The Juvenile Justice (Care and Protection of Children) Act, 2015 focuses primarily on the rehabilitation, social integration and protection of children in conflict with law, even amid the rapid expansion of digital technologies.

Recent data demonstrate an escalation in cyber offences involving children, including cyberbullying, the dissemination of explicit content, online harassment and identity misuse. This increase has expanded opportunities for both victimisation and offending. In spite of this transformation, the JJ Act remains largely offline-oriented, addressing traditional forms of delinquency while lacking specific recognition of cyber-enabled misconduct by juveniles.

C. Research objectives

The objective of this research is to examine the rise of cyber delinquency among children in India and to analyse whether the Juvenile Justice Act, 2015 adequately addresses cyber-enabled offences. The research further aims to identify legal and institutional gaps in addressing juvenile cyber misconduct and to evaluate international and technological approaches to juvenile cyber regulation. It proposes reforms integrating digital literacy and cyber accountability within juvenile justice frameworks.

D. Scope and limitations

The study focuses primarily on India's juvenile justice framework, analysing cyber offences committed by children in conflict with law and examining the statutory provisions of the Juvenile Justice Act, 2015. The scope is limited to legal and policy analysis and does not include

⁴ Jeong Ah Yoo, *What Shapes Cyber Delinquency in Adolescents?: A Holistic and Comparative Analysis of Cyber and Traditional Offline Delinquencies*, 136 CHILD. & YOUTH SERVS. REV. 106445 (2022), <https://doi.org/10.1016/j.childyouth.2022.106445>; see generally David P. Farrington, *Age and Crime*, 7 CRIME & JUST. 189 (1986), <https://doi.org/10.1086/449114>.

empirical fieldwork or psychological experimentation. International practices are referred to only for comparative understanding.

E. Review of literature

Existing Indian scholarship on juvenile justice largely examines cyber delinquency through the lens of socio-economic and psychological factors such as family environment, peer influence and lack of education, while analysing the Juvenile Justice (Care and Protection of Children) Act, 2015 as a welfare-oriented framework centred on rehabilitation and reintegration. Most legal studies, however, continue to address traditional contexts of juvenile offending, with limited attention to emerging forms of cyber delinquency.

Global research on children and cybercrime highlights the changing patterns of juvenile behaviour in digital environments. Psychological research explains that adolescence is marked by impulsivity, experimentation and sensitivity to peer validation, which are intensified in online spaces where young users often underestimate the permanence and legal consequences of digital actions.

II. RISE OF CHILD CYBER DELINQUENCY IN INDIA

Child cyber delinquency refers to juvenile misconduct committed through the use of the internet. It includes illegal or problematic behaviours by minors such as cyberbullying, hacking, fraud or creating obscene content. Data from the National Crime Records Bureau (NCRB) show that 65,893 cybercrime cases were registered in India in 2022, an increase of 24.4 per cent over the 52,974 cases registered in 2021, and that fraud was the motive in 64.8 per cent of them.⁵ The NCRB data also record 1,823 cases of cybercrime against children in 2022, up from 1,376 in 2021. These include 1,171 cases of publishing or transmitting material depicting children in sexually explicit acts, 158 cases of cyberstalking or bullying, and 416 other cyber-related offences.⁶ The upward trend has continued: 86,420 cybercrime cases were registered in 2023, an increase of 31.2 per cent over 2022.⁷

Merriam-Webster defines cybercrime as “criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data”.⁸

⁵ NAT'L CRIME RECORDS BUREAU, CRIME IN INDIA 2022, vol. 1, at xiv (2023).

⁶ Sarkar, *supra* note 2 (analysis of NCRB data by Child Rights and You); *see also* NAT'L CRIME RECORDS BUREAU, *supra* note 5, vol. 1, tbl. 4A.3 (1,171 cases of publishing or transmitting material depicting children in sexually explicit acts reported in 2022).

⁷ NAT'L CRIME RECORDS BUREAU, CRIME IN INDIA 2023, vol. 1, at xiv (2025).

⁸ MERRIAM-WEBSTER DICTIONARY, *Cybercrime*, <https://www.merriam-webster.com/dictionary/cybercrime> (last visited Oct. 13, 2026).

An analysis of State and Union Territory-wise cybercrime cases registered in India between 2021 and 2023 reveals an alarming escalation in reported offences. At the national level, total cases increased significantly over the three years (Figure 1), reflecting the rapid increase in digital activity and improved reporting practices. This surge, though remarkable, is concentrated in a few States, particularly Karnataka, Telangana, Uttar Pradesh and Maharashtra. These States account for a large and consistent share of total cases, with Karnataka and Telangana showing a steep increase by 2023. In contrast, the north-eastern States and smaller Union Territories continue to report very low case numbers, highlighting disparities in digital penetration and differences in law enforcement capacity. Notably, Bihar (from 1,413 cases in 2021 to 4,450 in 2023) and Kerala (from 626 to 3,295) have shown a sharp surge in reported cyber cases.⁹ These sudden rises may point to improved awareness of cyber offences or, conversely, to growing regional vulnerabilities. Overall, the data highlight the uneven nature of cybercrime in India. Regions with advanced internet penetration and digital adoption continue to record a large number of cases, placing a great burden on their law enforcement systems, whereas States with lower digital penetration report fewer cases, raising important concerns about regional readiness and policy capacity.

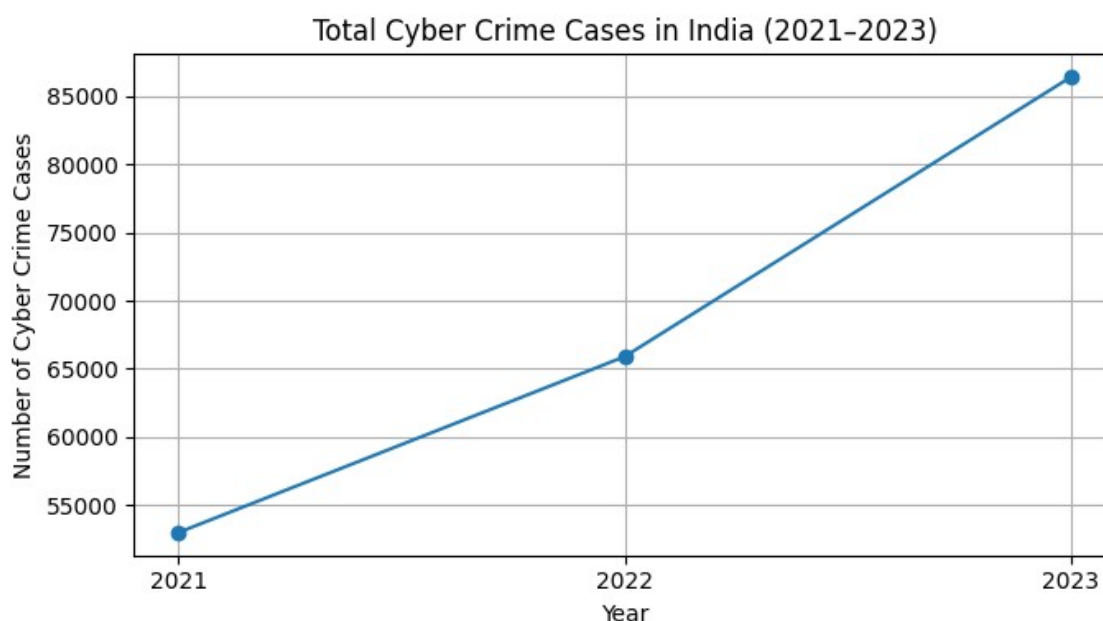


Figure 1: Total cybercrime cases registered in India, 2021–2023 (NCRB data: 52,974 in 2021; 65,893 in 2022; 86,420 in 2023)

⁹ NAT'L CRIME RECORDS BUREAU, *supra* note 7, vol. 2, ch. 9A (Cyber Crimes (States/UTs)); *Telangana, Karnataka Report Highest Cybercrime Cases Between 2021 and 2023*, SIASAT DAILY (Dec. 4, 2025), <https://www.siasat.com/telangana-karnataka-report-highest-cybercrime-cases-between-2021-and-2023-3308371/> (reporting the State-wise NCRB figures for 2021 to 2023 given in a written reply in the Rajya Sabha).

It is widely acknowledged that the actual number of cases is higher, since a large proportion of victims, especially women and children, are reluctant to report cases out of fear, social stigma or lack of knowledge about the reporting procedure.

The COVID-19 pandemic was a powerful accelerant of this boom in cyber cases. The pandemic thrust many children into digital spaces, forcing a shift to online learning and a greater use of digital media for entertainment and communication during confinement. Children's online exposure without parental supervision increased. The India Child Protection Fund reported that, according to data published by a major pornography website, traffic to that website from India rose by 95 per cent between 24 and 26 March 2020, in the first days of the nationwide lockdown, and claimed a steep rise in demand for child sexual abuse material, putting children at increased risk and vulnerability.¹⁰

III. DIFFERENT TYPES OF CYBERCRIME

A. Cyberstalking

The *Oxford Advanced Learner's Dictionary* defines “stalk” as “to illegally follow and watch somebody over a long period of time, in a way that is annoying or frightening”. Cyberstalking occurs when a person is continuously followed and harassed online. As Sameer Hinduja explains, it involves the use of technology “to make someone else afraid or concerned about their safety”; such conduct “is threatening or otherwise fear-inducing, involves an invasion of a person's relative right to privacy, and manifests in repeated actions over time”.¹¹

Typical cyberstalking behaviours, as Hinduja describes them, include tracking down a person's private information and using it to frighten them, letting the person know that they are being watched, and following their social media accounts to find out where they are in order to turn up uninvited; such conduct is meant to instil fear and agitation.

B. Cyberbullying

Cyberbullying is “bullying that takes place over digital devices like cell phones, computers, and tablets”, and it “can occur through SMS, Text, and apps, or online in social media, forums, or

¹⁰ *Demand for Child Pornography Rises Steeply in India amid COVID-19 Lockdown*, THE WEEK (Apr. 13, 2020), <https://www.theweek.in/news/india/2020/04/13/demand-for-child-pornography-rises-steeply-in-india-amid-covid-19-lockdown.html> (reporting INDIA CHILD PROTECTION FUND, CHILD SEXUAL ABUSE MATERIAL IN INDIA (2020)).

¹¹ OXFORD ADVANCED LEARNER'S DICTIONARY, *Stalk* (verb), https://www.oxfordlearnersdictionaries.com/definition/english/stalk_2 (last visited Oct. 13, 2026); Sameer Hinduja, *Cyberstalking*, CYBERBULLYING RESEARCH CENTER, <https://cyberbullying.org/cyberstalking> (last visited Oct. 13, 2026).

gaming where people can view, participate in, or share content”.¹² It includes the use of electronic media for covert psychological bullying by sending or posting threatening or frightening messages.

C. Child pornography

This refers to criminal offences comprising internet-related sex crimes and the visual depiction of a minor engaged in sexually explicit activity.

The invention of digital devices such as cameras and phones, and subsequent technological advances, have provided new avenues for the exploitation of children by facilitating the distribution of pictorial representations of them.

Commercial child pornography persuades child victims that sexual activities are fun and exciting, making them feel that such activity is acceptable in society and exploiting their curiosity. These sites contain pictures and videos of children viewing pornography, which further exert a harmful influence on minors. The growth of such material is driven by improvements in technology, which allow videos and photos to circulate at much lower cost and in higher quality, encouraging people to engage in such crimes.

D. Cyber terrorism

Cyber terrorism involves the use of cyberattacks to cause fear and disruption for political or social ends, targeting critical infrastructure such as power grids, finance and transport. Such attacks use tools like DDoS, phishing and malware, and constitute a major global threat requiring strong legal frameworks for both prevention and prosecution. India addresses it in the Information Technology Act, 2000, although the definition and scope of the offence remain debated. Section 66F of the IT Act specifically addresses cyber terrorism: it punishes, with imprisonment which may extend to imprisonment for life, acts done with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people, by denying authorised access to a computer resource, accessing a computer resource without authorisation, or introducing a computer contaminant, where the conduct causes or is likely to cause death or injury, damages property, disrupts supplies or services essential to the life of the community, or adversely affects critical information infrastructure.¹³

¹² U.S. DEP'T OF HEALTH & HUM. SERVS., *What Is Cyberbullying*, STOPBULLYING.GOV, <https://www.stopbullying.gov/cyberbullying/what-is-it> (last visited Oct. 13, 2026).

¹³ The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), § 66F [hereinafter IT Act] (inserted by the Information Technology (Amendment) Act, No. 10 of 2009).

Examples of cyber terrorism include hacking communication systems to spread threats, disrupting financial institutions, introducing viruses into vital data networks and causing large-scale disruption of computer networks.

E. Continuous and unwanted exposure to sexually explicit content

This is a widespread online problem, especially for young people. Exposure often occurs accidentally on the internet and is linked to increasing sexual curiosity, sensation-seeking and reduced parental monitoring; it poses risks to psychological well-being and influences sexual attitudes and behaviour. The rapidly escalating exposure to internet pornography has harmful effects not only on adolescents but also on young people and society as a whole. Such exposure has been associated with vulnerabilities that include delinquent tendencies, depression, interpersonal victimisation and post-traumatic stress disorder.

F. Hacking

Hacking is “the use of unconventional or illicit means to gain unauthorized access to a digital device, computer system or computer network”. Malicious hacking now sustains a large criminal economy: offenders profit from cyberattacks, from extortion and from trading malware and stolen data among themselves. Individuals may suffer identity theft and financial loss, while organisations may face system outages and data breaches that cost them customers, revenue and reputation and expose them to fines or other legal sanctions.¹⁴

G. Intellectual property crimes

Intellectual property refers to “creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce”. Its principal categories include patents, copyright, trademarks, industrial designs, geographical indications and trade secrets.¹⁵

Intellectual property crime involves the illegal use, theft or distribution of protected creations, often through the manufacture and sale of counterfeit physical goods or the illegal sharing of digital content for profit.

The impacts of intellectual property crime include the following:

1. It leads to lost revenue, jobs and tax income for businesses and governments.

¹⁴ Matthew Kosinski, *What Is Hacking?*, IBM THINK, <https://www.ibm.com/think/topics/cyber-hacking> (last visited Oct. 13, 2026).

¹⁵ WORLD INTELL. PROP. ORG., *What Is Intellectual Property?*, <https://www.wipo.int/about-ip/en/> (last visited Oct. 13, 2026); see also WORLD INTELL. PROP. ORG., WIPO INTELLECTUAL PROPERTY HANDBOOK: POLICY, LAW AND USE (2d ed. 2004) (WIPO Pub. No. 489(E)).

2. Counterfeit products can be dangerous or deadly.
3. It discourages investment in new ideas and development.

H. Phishing

Phishing is a deceptive cyberattack in which attackers impersonate trusted entities through email, text messages or websites to trick individuals into revealing sensitive information such as passwords, credit card numbers or Social Security numbers. It is a technique for deceitfully gaining access to private information. A phisher typically sends an email or creates a website purporting to be from the victim's bank or credit card company, asking the victim to fill in an online form disclosing an ATM card PIN, a one-time password (OTP) or a home address.

Common phishing techniques include spear phishing, whaling, URL spoofing or link manipulation, and AI-assisted social engineering.

IV. CAUSES AND CONTRIBUTING FACTORS

A. Digital environment and adolescent vulnerability

The internet has become one of the most influential elements of everyday life, functioning as a primary space for social interaction, entertainment and identity exploration. Adolescents today engage with digital platforms across multiple contexts, making online environments inseparable from their offline experiences. In India, 83 per cent of children aged 10 to 14 use smartphones, seven percentage points above the international average of 76 per cent.¹⁶ The same McAfee study found that Indian children have the highest online risk exposure and are the youngest to reach mobile maturity.¹⁷ This shows the extent to which adolescents grow up surrounded by the internet and digital platforms, and this exposure strongly shapes how they think, feel and behave. The internet is a vast and diverse realm, offering a wide array of information and entertainment resources, including gaming, which cater to the intellectual curiosity and knowledge-seeking propensities of adolescents. As a result, the internet has become a dominant setting within which the adolescent develops and grows.

Early adolescence, in particular, is a critical and vulnerable developmental phase, marked by heightened emotional reactivity and ongoing neurological maturation. Adolescents become especially susceptible to the digital environment because of their increasing sensitivity to external influence and social cues.

¹⁶ McAfee, *supra* note 3.

¹⁷ *Id.*

B. Problem behaviour theory and juvenile delinquency

Problem behaviours are persistent patterns of conduct that interfere with a child's learning, communication and relationships, and that harm both the child and the people around the child. They may be overt, such as tantrums or aggression, or less visible, such as prolonged crying, and if left unaddressed they can impede the child's development. In adolescence, problem behaviours are particularly salient because of the rapid biological, psychological and social changes occurring during this period.

Problem behaviours are classified into two categories: internalising and externalising behaviours. Internalising behaviours are directed inward and include emotional and psychological difficulties such as anxiety, depression and social withdrawal. Externalising behaviours, in contrast, are directed outward and manifest through actions such as aggression, rule-breaking, truancy and substance use.

The consequences of problem behaviour in children include academic decline, strained peer and family relations, emotional distress and long-term risks to digital citizenship.

Juvenile cyber delinquency can be conceptualised as an extension of externalising behaviour, involving tendencies such as aggression, impulsivity, rule-breaking and low self-control, often transferred from offline contexts to digital space. The key to understanding it is to examine the environmental conditions that facilitate these expressions. The internet is a major part of this external context, offering conditions that can heighten and activate pre-existing problem behaviour tendencies among adolescents.

C. Multilevel contributing factors underlying internet-related juvenile delinquency**i. Individual-level factors**

These include impulsivity and poor self-control, which increase risky online actions and rule-breaking behaviours. Other factors include anxiety, stress and frustration, which often lead to online aggression and deviant coping mechanisms.

ii. Family-related factors

A lack of parental monitoring or digital supervision, weak parent-child attachment, and family conflict or neglect allow unrestricted internet access and push adolescents towards maladaptive online environments.

iii. Peer and social factors

Peer influence plays a major role in today's generation. Peers influence children, increase their vulnerability in online spaces and normalise cyber deviance. Such conduct in adolescents arises from a constant desire for social approval or status, especially in digital settings.

iv. Digital and environmental factors

Increased access to digital spaces has lowered the fear of consequences because of the anonymous nature of online activity and reduced accountability online. These factors lead to easy access to harmful content, algorithmic reinforcement and excessive screen time, which displace prosocial offline activities and amplify deviant interests such as violence, pornography and illegal activities.

v. Broader contextual factors

In today's generation, school disengagement and academic stress have increased vulnerability to online delinquency, while socio-economic disadvantage limits access to structured supervision and support.

D. Case studies

i. Gurugram case (2020)

A 17-year-old boy from Gurugram, India, died by suicide after a girl accused him of sexual harassment in an Instagram story. He took his own life in May 2020. He was bullied, shamed and threatened after the allegation was posted on Instagram. Despite the absence of any formal complaint or verification, the allegation circulated rapidly online, leading to sustained cyberbullying, threats and public shaming. The online attacks escalated and caused him overwhelming psychological distress. His family maintained that the allegation was false and sought a police inquiry into the online harassment and trolling that preceded his death.¹⁸ The case illustrates the irreversible harm that unregulated online mob behaviour can cause.

This case shows how cyberbullying by children can escalate rapidly, and how perceived anonymity and a lack of consequences can lead adolescents to engage in harmful online conduct. Existing legal frameworks, including the Juvenile Justice Act, 2015, remain reactive rather than preventive, which underlines the need to strengthen the limited safeguards against psychological harm caused by online abuse. This exposes a regulatory and institutional gap:

¹⁸ *Gurugram Teen Suicide Case: Parents Seek Probe Against Minor Girl*, THE QUINT (May 8, 2020), <https://www.thequint.com/news/india/boys-locker-room-gurugram-teen-boy-suicide-parents-file-complaint-against-minor-girl>.

while the law identifies children as victims of cybercrime, it often fails to address situations in which children themselves are the perpetrators of cyber harm.

ii. Ujjain case (2023)

A 16-year-old Instagram content creator from Ujjain, Madhya Pradesh, posted a reel during Diwali in which they appeared in a saree. The reel was flooded with thousands of hate-filled, homophobic and derogatory comments targeting the teenager's identity and appearance. The comments were abusive in nature and trolled the teenager for self-expression online. Nine days after posting the video, amid widespread online harassment, the teenager died by suicide in November 2023. Members of the LGBTQ+ community and activists voiced grief and concern and called for stringent measures against cyberbullying on social media platforms, highlighting how relentless online hate can affect young people's mental health and safety.¹⁹

This case illustrates how problem behaviour tendencies among online users (for example, hostile commenting, harassment and hate speech) are expressed as cyber delinquent acts that can seriously affect adolescent well-being. The continuous online trolling and abuse reflect a form of cyber delinquency in which social media becomes a space for belligerent behaviour that contributes to emotional anguish and distress.

V. LEGAL FRAMEWORK GOVERNING JUVENILE CYBER OFFENCES IN INDIA

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

The Juvenile Justice (Care and Protection of Children) Act, 2015 establishes the main justice framework for children, providing for children in conflict with law and children in need of care and protection. India's first comprehensive juvenile justice legislation, the Juvenile Justice Act, 1986, received the President's assent on 1 December 1986. It was replaced by the Juvenile Justice (Care and Protection of Children) Act, 2000, which was in turn replaced by the 2015 Act. The 2015 Act was most recently amended in 2021, with effect from 1 September 2022.²⁰

i. Objectives

The Act's main objectives are to ensure the care, protection, development, treatment and social reintegration of children in conflict with law and children in need of care and protection through

¹⁹ *Teen Queer Artist Kills Self After Receiving Homophobic Comments on Instagram*, DECCAN HERALD (Nov. 26, 2023), <https://www.deccanherald.com/india/madhya-pradesh/teen-queer-artist-kills-self-after-receiving-homophobic-comments-on-instagram-2785500>.

²⁰ The Juvenile Justice (Care and Protection of Children) Act, No. 2 of 2016, INDIA CODE (2016) [hereinafter JJ Act], amended by The Juvenile Justice (Care and Protection of Children) Amendment Act, No. 23 of 2021, INDIA CODE (2021); see also The Juvenile Justice Act, No. 53 of 1986, INDIA CODE (1986) (repealed); The Juvenile Justice (Care and Protection of Children) Act, No. 56 of 2000, INDIA CODE (2000) (repealed).

a child-friendly justice system. It prioritises the best interests of the child and gives effect to the standards of the United Nations Convention on the Rights of the Child (UNCRC).²¹

ii. Purpose

The Act was introduced to establish a child-friendly system both for the care and protection of vulnerable children and for the handling of children who have committed offences. It focuses on reform and social reintegration and aims to provide appropriate care, safety and rehabilitation. It also seeks greater accountability by allowing children aged 16 to 18 to be tried as adults for heinous offences.

iii. Meaning of juvenile

In common usage, “juvenile” describes anything characteristic of or relating to children or young people, often implying immaturity.

Under the Juvenile Justice Act, 2015, a “juvenile” is a child below the age of eighteen years, and a “child” is a person who has not completed eighteen years of age.²²

iv. Categories of offences

The JJ Act classifies offences into three categories:²³

1. Petty offences, for which the maximum punishment is imprisonment for up to three years.
2. Serious offences, which are punishable with a minimum term of imprisonment of more than three years and not exceeding seven years, or with a maximum term of more than seven years where no minimum term, or a minimum term of less than seven years, is provided.
3. Heinous offences, for which the minimum punishment is imprisonment for seven years or more.

v. Constitution of Juvenile Justice Boards

Section 4 of the JJ Act requires the State Government to constitute one or more Juvenile Justice Boards (JJBs) for every district to deal with children in conflict with law.²⁴ Juvenile Justice Boards are quasi-judicial bodies responsible for conducting inquiries into offences committed

²¹ JJ Act pmb.; Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

²² JJ Act § 2(12), (35).

²³ *Id.* § 2(33), (45), (54) (cl. (54) as substituted by the Juvenile Justice (Care and Protection of Children) Amendment Act, No. 23 of 2021, with effect from Sept. 1, 2022).

²⁴ *Id.* § 4(1).

by juveniles, evaluating mental and physical capacity, determining rehabilitative measures and ensuring child-friendly procedures.

vi. Preliminary assessment of heinous offences

Section 15 requires the Juvenile Justice Board to conduct a preliminary assessment where a child who has completed or is above the age of sixteen years is alleged to have committed a heinous offence.

The Board assesses the child's mental and physical capacity to commit the offence, the child's ability to understand its consequences, and the circumstances in which it was allegedly committed. On the basis of this assessment, the Board may either dispose of the matter itself or order the transfer of the trial to the Children's Court, which then decides whether the child should be tried as an adult.²⁵

Section 15 raises crucial concerns in cyber cases, such as the complicated assessment of intent in offences that involve high technical ability but immature risk perception, and the question whether a child truly understood the long-term digital consequences of an act, which are difficult to determine given their indirect nature.

vii. Limitations in cyber matters

Although Juvenile Justice Boards are the principal forum for children in conflict with law in India, they face serious structural challenges in cyber matters:

1. **Lack of technical expertise.** Cyber offences require an understanding of technological processes, online platforms and digital network chains, which usually fall outside the traditional expertise of the Board. Boards need to build technological expertise because cyber offences involve digital forensics and complex evidence.
2. **Inadequate specialised training.** Cyber delinquency differs from regular offending because it often arises from curiosity, peer influence or experimentation rather than *mens rea* (criminal intent). Members of Juvenile Justice Boards often lack specialised training in cybercrime dynamics or digital behaviour, a gap that results either in the over-criminalisation of children or in a failure to address the underlying behavioural causes.
3. **Absence of digital rehabilitation frameworks.** Existing rehabilitation and correctional programmes typically focus on behavioural counselling, education or vocational training, which are largely designed for offline offences and do not

²⁵ *Id.* §§ 15(1)–(2), 18(3), 19(1).

adequately address online misconduct. Boards need to include digital literacy, responsible technology use and cyber ethics training to address the root of these forms of delinquency.

4. **Difficulty in assessing intent and harm.** Children may perceive actions such as hacking, online trolling or data misuse as harmless experimentation, with no knowledge of the consequences. Cyber offences often lack visible or direct harm, making the assessment of *mens rea* complicated and slow.
5. **Jurisdictional and evidentiary challenges.** Cyber offences often involve cross-border platforms, anonymous identities and digital evidence stored on remote servers. Delays or evidentiary complications may prolong proceedings, undermining the child-friendly and expeditious inquiry process envisaged by the JJ Act.

B. The Information Technology Act, 2000

The Information Technology Act governs cyber offences such as hacking and unauthorised access, identity theft, cyber fraud, the publication of obscene content, online harassment and data misuse.²⁶ It provides substantive offences and penalties for cyber misconduct.

A difficulty with the IT Act is that its provisions do not distinguish between adults and juveniles, so that the punishments it prescribes may be disproportionate for minors. The JJ Act functions as special legislation for juveniles; its provisions apply to all matters concerning children in conflict with law notwithstanding anything in any other law, so its procedures prevail even when an offence arises under the IT Act.²⁷

VI. CRITICAL ANALYSIS: GAPS IN THE JUVENILE JUSTICE ACT

The Juvenile Justice (Care and Protection of Children) Act, 2015 establishes a comprehensive framework for dealing with children in conflict with law, grounded in the principles of rehabilitation and social reintegration. However, the statutory structure concentrates heavily on traditional forms of juvenile offending, such as theft and violence, and contains no provisions specifically addressing cyber offences or digitally mediated misconduct.

In practice, juvenile delinquency has moved increasingly into online spaces, where offences differ fundamentally from conventional ones because they are facilitated by anonymity, technological accessibility and a reduced perception of harm.

²⁶ IT Act §§ 43, 66, 66C, 66D, 66E, 67, 67A, 67B.

²⁷ JJ Act § 1(4).

The lack of cyber-specific provisions creates a normative gap, requiring the law to interpret digitally complex conduct through frameworks designed for physical crimes. Consequently, the developmental and behavioural characteristics associated with online offending are often not accounted for in the legal response.

This gap undermines the reformative objectives of juvenile justice. The lack of statutory recognition of cyber delinquency reflects a structural misalignment between evolving forms of juvenile offending and existing legal responses.

A. Inadequate digital maturity assessment

Cyber delinquency often involves a paradoxical situation in which juveniles' lack of emotional maturity or awareness of legal consequences creates a dangerous environment. Section 15 of the JJ Act introduces a preliminary assessment mechanism for children, focusing on mental and physical capacity and the ability to understand the consequences of the offence. Although it attempts to distinguish between immature conduct and criminal intent, it does not account for the particular characteristics of cyber offences.

The absence of a framework for assessing digital maturity creates a risk of inaccurate attribution of culpability, in which juveniles may be perceived as more responsible than they actually are, leading to harsher procedural outcomes that conflict with the core philosophy of juvenile justice.

B. Investigative challenges

Digital offences require specialised skills in electronic evidence collection, data preservation and cyber forensic analysis. However, the agencies that investigate cases involving juveniles lack adequate technological capacity and specialised training, which presents technical challenges extending beyond conventional policing methods.

C. International comparative analysis

This section examines selected jurisdictions that have incorporated digital realities into their juvenile justice systems. The comparative analysis shows how child-centric justice systems adapt to emerging forms of cyber delinquency through rehabilitative interventions focused on digital behaviour.

i. United Kingdom

In England and Wales, the youth justice system is overseen by the Youth Justice Board (YJB), which monitors local youth justice services and promotes a "Child First", rehabilitative approach to offending by children; it has recently recognised online harms, including

problematic online behaviour by children, as calling for early, co-ordinated responses that avoid unnecessary criminalisation.²⁸

Local safeguarding practice relies on multi-agency working, in which education, health, social care and police professionals jointly assess and respond to harm to children, including harm arising online.²⁹ The National Crime Agency's Cyber Choices programme, delivered by regional Cyber Choices teams, seeks to divert young people from cyber offending by encouraging them to make informed choices in their use of technology and by raising awareness of the Computer Misuse Act 1990.³⁰ Mechanisms such as Youth Inclusion and Support Panels (YISPs), developed by the YJB and piloted from 2003 for children aged 8 to 13, were designed to identify children at risk of offending and to intervene early through behavioural and social support.³¹

The UK approach demonstrates a shift towards preventive and risk-management frameworks. Rather than creating separate cyber-specific juvenile courts, the system integrates such cases into broader youth justice risk assessments. This approach emphasises early intervention, behavioural correction and safeguarding rather than criminalisation.

ii. Singapore

Singapore's juvenile justice system places strong emphasis on rehabilitation and structured correctional programming under the Children and Young Persons Act.³² Youth offenders are generally dealt with by the Youth Courts, which focus on rehabilitation; the system emphasises repairing harm and reintegrating the child into society rather than mere punishment.

Efforts include school programmes and campaigns to educate young people about cyberbullying, online safety and the legal consequences of digital actions. While rehabilitation is preferred, serious offences can lead to fines, probation or detention in a juvenile home.

Singapore's approach reflects a preventive and technological orientation, in which juvenile offending in digital spaces is addressed through behavioural reform and digital literacy.

²⁸ YOUTH JUSTICE BD. FOR ENG. & WALES, STRATEGIC PLAN 2024–27 (2024), <https://www.gov.uk/government/publications/youth-justice-board-for-england-and-wales-strategic-plan-2024-27>; Press Release, YOUTH JUSTICE BD. FOR ENG. & WALES, *New Evidence on Online Harms Affecting Children* (June 25, 2026), <https://www.gov.uk/government/news/new-evidence-on-online-harms-affecting-children>.

²⁹ HM GOV'T, WORKING TOGETHER TO SAFEGUARD CHILDREN: A GUIDE TO INTER-AGENCY WORKING TO SAFEGUARD AND PROMOTE THE WELFARE OF CHILDREN (2018).

³⁰ NAT'L CRIME AGENCY, *Cyber Choices*, <https://www.nationalcrimeagency.gov.uk/cyber-choices> (last visited Oct. 13, 2026).

³¹ JANET WALKER ET AL., YOUTH INCLUSION AND SUPPORT PANELS: PREVENTING CRIME AND ANTISOCIAL BEHAVIOUR? EXECUTIVE SUMMARY (Dep't for Children, Schs. & Families Research Report DCSF-RW018, 2007), <https://www.gov.uk/government/publications/youth-inclusion-and-support-panels-preventing-crime-and-anti-social-behaviour-executive-summary>.

³² Children and Young Persons Act 1993 (Cap. 38) (Sing.).

iii. New Zealand

New Zealand's youth justice system is grounded in the Oranga Tamariki Act 1989, which prioritises family and community involvement in responding to youth offending.³³ New Zealand's approach to cybersecurity literacy among young people focuses on strengthening resilience and awareness through national frameworks,³⁴ but arguably faces challenges because of its reliance on technical solutions rather than education-driven behavioural change.

A central mechanism is the family group conference (FGC), in which the offender, family, victim and professionals collectively decide on accountability and rehabilitation measures. It is particularly relevant to cyber offences because online harm involves peer relationships, reputational damage and emotional consequences rather than purely physical injury.

VII. RECOMMENDATIONS AND DIGITAL-AGE REFORMS

A. Reforms in the Juvenile Justice Act, 2015

The Juvenile Justice Act, 2015 was framed around a largely pre-digital understanding of juvenile offending as physical or situational. The nature of juvenile offending has been altered by the emergence of cyber delinquency, where offences are more anonymous, scalable and psychologically detached from immediate consequences.

International programmes emphasise that legal frameworks must combine accountability with digital education and prevention, rather than relying on purely punitive responses.

The recommended reforms include inserting a separate chapter or explanation recognising cyber offences by children, introducing mandatory cyber-awareness counselling before adjudication, and allowing diversion programmes for first-time cyber offenders.

B. Cyber-specialised Juvenile Justice Boards

Digital crimes involve electronic evidence, platform jurisdiction, data recovery timelines and online psychological behaviour. However, Juvenile Justice Boards currently deal with cyber offences without specialised technical understanding. India faces an enforcement deficit, including a limited number of trained cyber personnel and limited investigative capacity, which affects outcomes in cases involving minors.

This highlights the need to establish cyber-specialised Juvenile Justice Boards in metropolitan districts, which should include cyber forensic experts, child psychologists and digital safety

³³ Oranga Tamariki Act 1989 (N.Z.).

³⁴ N.Z. GOV'T, THE DIGITAL STRATEGY FOR AOTEAROA (2022), <https://www.digital.govt.nz/dmsdocument/237~the-digital-strategy-for-aotearoa/html>.

counsellors. This would shift the approach from punishment to understanding why the offence occurred.

C. Digital maturity and behaviour assessment

Cyber delinquency requires nuanced evaluation. While traditional juvenile assessment evaluates age, intent and physical circumstances, cyber delinquency requires evaluation of online peer pressure, gaming or social media addiction, understanding of privacy and consent, and awareness of digital permanence.

The study therefore recommends a Digital Behaviour Assessment Report (DBAR) to assess the child's level of digital literacy, exposure to harmful online communities and impulsivity indicators, and awareness of legal consequences.

D. Cyber-specific rehabilitation programmes

Current rehabilitation programmes focus on vocational skills and behavioural counselling but rarely address digital behaviour. Global youth cybercrime prevention programmes emphasise building resilience, digital awareness and responsible online participation rather than isolating children from technology.

This can be reformed through mandatory modules on cyber ethics, consent and privacy, online accountability and digital footprint awareness.

E. Training for law enforcement and child protection agencies

Inadequate investigative capacity is one of the most significant structural weaknesses in addressing child cyber delinquency. Limited cybercrime training among investigating officers and insufficient digital forensic infrastructure lead to delayed investigations and weak evidence handling. Cases collapse because of procedural lapses when officers are not trained, which can also lead to children being wrongly criminalised. Recommended reforms include mandatory cybercrime certification for officers dealing with juveniles, and standard operating procedures for device seizure, digital evidence preservation and interaction with minors.

VIII. CONCLUSION

The internet has created opportunities for education, creativity and communication, while simultaneously contributing to the emergence of new forms of juvenile delinquency that operate beyond traditional legal and institutional understanding. The rapid expansion of digital technology has fundamentally transformed the social and virtual environment in which children grow, learn and interact. The rise in cyberbullying, identity misuse, online harassment and

exposure to harmful digital spaces is compounded by the lack of specific mechanisms to respond to cyber-enabled misconduct among children.

The Juvenile Justice (Care and Protection of Children) Act, 2015 was designed within a framework that primarily addressed conventional forms of delinquency. The absence of cyber-specific assessment tools, preventive education models and specialised investigative procedures creates a gap between the Act's rehabilitative objectives and their realisation in cyber cases. Moreover, inadequate awareness among children of privacy, consent and legal consequences further contributes to the increase in cyber delinquency.

Addressing this challenge requires a shift from purely punitive or reactive approaches to preventive and reformatory strategies. Ultimately, an effective juvenile justice system in the digital era must recognise that child cyber delinquency is not merely a legal issue but a developmental and societal concern.
