

Juvenile Delinquency in the Digital Age: Technology, Social Media and Emerging Challenges in Indian Juvenile Justice

Dr. Keval Ukey ^{1*}, Sri. Bhuwan ¹

¹ Ph.D. (Law) Research Scholar, School of Law, Lingaya's Vidyapeeth, Faridabad,

Email ID: pbbhuwan2011@gmail.com

Corresponding Author

Dr. Keval Ukey *

Email ID : kevalukey@gmail.com

Abstract

This research examines the growing relationship between technology, social media and juvenile delinquency in India and its emerging implications for the juvenile justice system. The widespread use of smartphones, social networking platforms, online gaming and digital communication has created new opportunities for education and social interaction but has also exposed children to cyberbullying, online exploitation, identity misuse, cybercrime, harmful content and technology-facilitated offending. The study critically examines whether the existing juvenile justice framework, particularly the Juvenile Justice (Care and Protection of Children) Act, 2015, is adequately equipped to address offences involving digital technologies while protecting the rights, privacy and developmental interests of children. It further considers the challenges faced by law-enforcement agencies, Juvenile Justice Boards and other institutions in identifying, investigating and responding to technology-related juvenile offending, including issues of digital evidence, online anonymity and rapidly changing technologies.

The research adopts a socio-legal approach, analysing statutory provisions, judicial developments, official crime data and relevant child-rights standards. It argues that an effective response requires a balanced approach combining accountability with digital literacy, prevention, rehabilitation, restorative justice and protection of children's fundamental rights. The study proposes strengthening the capacity of the juvenile justice system to respond to emerging forms of technology-related delinquency without adopting excessively punitive measures that may undermine the rehabilitative objectives of juvenile justice.....

Keywords: Technology; Social Media; Juvenile Delinquency; Cybercrime; Children in Conflict with Law; Juvenile Justice; Cyberbullying; Digital Evidence; Child Rights; Rehabilitation.

INTRODUCTION

Being a professional athlete is necessarily time-bound: the years of active, competitive participation, and the identity, daily routines, and physiological training that characterise athletes' lives, are usually over well before midlife, after which life takes place. The rapid expansion of smartphones, social media, online gaming and digital communication has significantly transformed the social environment in which children and adolescents grow and interact. Technology provides children with opportunities for education, communication, creativity and access to information, but it has simultaneously created new forms of vulnerability and technology-facilitated offending. Children may become victims or perpetrators of cyberbullying, online harassment, identity misuse, fraud, sexual exploitation and other forms of cyber-related misconduct. The National Commission for Protection of Child Rights (NCPCR), in its study on the physical, behavioural and psychosocial effects of internet-accessible devices on children, found that internet-enabled devices have become an important part of children's daily lives, with online classes, messaging applications, educational material, music and gaming among their major uses.¹

The emergence of technology-related juvenile delinquency presents a new challenge for India's juvenile justice system because traditional concepts of juvenile offending are increasingly intersecting with the digital environment. The conduct of a child online may involve complex questions concerning anonymity, digital evidence, privacy, jurisdiction and the distinction between harmful behaviour and criminal conduct. Consequently, the juvenile justice framework must respond to technology-related offences while preserving its fundamental emphasis on child protection, rehabilitation and reintegration. International child-rights standards recognise that the digital environment affects the exercise of children's rights and require States to protect children

¹ National Commission for Protection of Child Rights, Effects (Physical, Behavioural and Psycho-Social) of Using Mobile Phones and Other Devices with Internet Accessibility by Children (2022).

from online risks while respecting their privacy, freedom of expression, access to information and evolving capacities.²

2. Technology and the Changing Nature of Juvenile Delinquency

Technology has altered both the opportunities and methods through which juvenile delinquency can occur. Earlier forms of juvenile offending were generally associated with physical or community-based activities, whereas digital platforms enable conduct to take place remotely, anonymously and across geographical boundaries. Social-media platforms, messaging applications, online games and other digital services may facilitate cyberbullying, online threats, harassment, impersonation, cyber fraud, unauthorised access and the circulation of harmful or unlawful material. The digital environment can also enable peer influence to operate continuously beyond the school or neighbourhood, making it more difficult for parents, teachers and authorities to identify problematic behaviour at an early stage.

The changing nature of juvenile delinquency also requires a distinction between children who deliberately engage in criminal conduct and children whose online behaviour results from peer pressure, inadequate digital awareness, experimentation or limited understanding of the consequences of digital actions. The NCPCR's study demonstrates the extensive use of internet-enabled devices by children and highlights the importance of understanding children's behavioural and psychosocial relationship with technology rather than treating technology merely as a source of criminality. A rights-based response should therefore combine prevention, digital literacy, parental and institutional guidance, proportionate legal intervention and rehabilitation. This approach is consistent with the international principle that children must be protected from harmful digital environments while also being enabled to participate safely and meaningfully in the digital world.³

3. Social Media and Juvenile Delinquency in India

Social media has become an important part of adolescent communication and peer interaction, creating both positive opportunities and new risks. The NCPCR study found that messaging applications were among the purposes for which children use smartphones and internet-enabled devices, alongside education, study materials, music and games. The constant connectivity associated with social media can expose children to cyberbullying, online humiliation, peer pressure, harmful content and potentially exploitative interactions. At the same time, the digital environment may allow children to participate in harmful conduct without fully understanding the permanence, reach or consequences of their actions. These circumstances make digital literacy and early intervention important components of contemporary child protection and juvenile justice policy.⁴

From a legal perspective, social-media-related juvenile delinquency creates a difficult balance between protecting children and respecting their fundamental rights. Measures addressing harmful online behaviour must take account of children's privacy, dignity, freedom of expression, access to information and evolving capacities while ensuring protection from exploitation and abuse. General Comment No. 25 emphasises that States should protect children from harmful content and online risks while respecting their rights in the digital environment and strengthening digital literacy among children, parents and educators. Accordingly, India's response to social-media-related juvenile delinquency should not be confined to criminal enforcement; it should integrate child protection, cyber-safety education, responsible digital use, family and school intervention, restorative approaches and rehabilitation within the existing juvenile justice framework.⁵

² U.N. Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (2021).

³ National Commission for Protection of Child Rights, Effects (Physical, Behavioural and Psycho-Social) of Using Mobile Phones and Other Devices with Internet Accessibility by Children (2022); U.N. Committee on the Rights of the Child, General Comment No. 25 (2021), U.N. Doc. CRC/C/GC/25.

⁴ National Commission for Protection of Child Rights, Effects (Physical, Behavioural and Psycho-Social) of Using Mobile Phones and Other Devices with Internet Accessibility by Children (2022).

⁵ U.N. Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (2021).

4. Empirical Analysis of Cybercrime and Juveniles in India

The empirical analysis of technology-related juvenile delinquency must begin with the broader growth of cybercrime in India. The National Crime Records Bureau (NCRB), *Crime in India 2023* recorded 86,420 cybercrime cases in 2023, compared with 65,893 cases in 2022, representing an increase of 31.2%. The cybercrime rate also increased from 4.8 to 6.2 per lakh population. Importantly, NCRB data do not provide a separate national category identifying the age of every accused in cybercrime cases; therefore, cybercrime statistics should not be incorrectly presented as statistics of juvenile cyber offenders. They are used here to establish the rapidly expanding digital-crime environment within which children and adolescents may be involved either as offenders or victims.⁶

Table 1: Growth of Cybercrime in India

Year	Cybercrime Cases	Change
2021	52,974	-
2022	65,893	+24.4%
2023	86,420	+31.2%

Source: NCRB, *Crime in India 2023*. The Ministry of Home Affairs has also reproduced the NCRB State/UT-wise figures for 2021-2023.

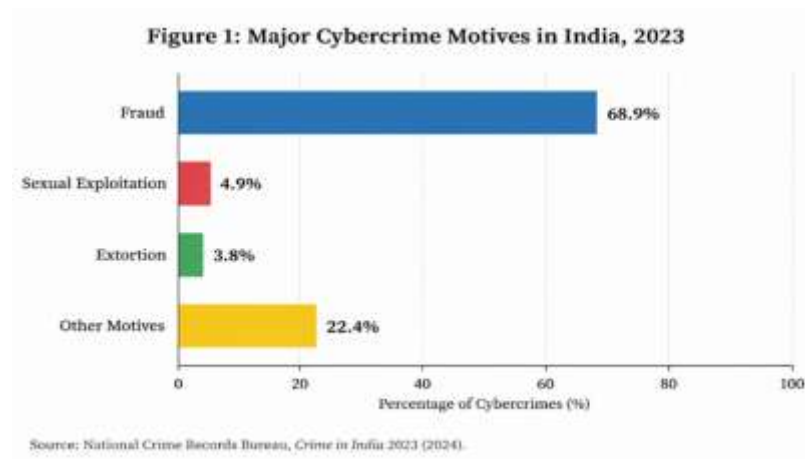
The nature of cybercrime recorded by NCRB indicates that fraud is the dominant motive. In 2023, 59,526 cases, or approximately 68.9% of all reported cybercrime cases, were recorded with fraud as the motive. Sexual exploitation accounted for 4,199 cases (4.9%), while extortion accounted for 3,326 cases (3.8%). This pattern demonstrates that the digital environment is increasingly being used for financially motivated and exploitative conduct. For juvenile justice research, these trends are significant because adolescents may encounter such activities through peer networks, gaming communities, social-media groups and other online environments, either as victims, facilitators or offenders.⁷

Table 2: Major Motives of Cybercrime, 2023

Motive	Cases	Approx. %
Fraud	59,526	68.9%
Sexual Exploitation	4,199	4.9%
Extortion	3,326	3.8%
Other motives	19,369	22.4%
Total	86,420	100%

⁶ National Crime Records Bureau, Ministry of Home Affairs, Government of India, *Crime in India 2023*, Vol. II (2025).

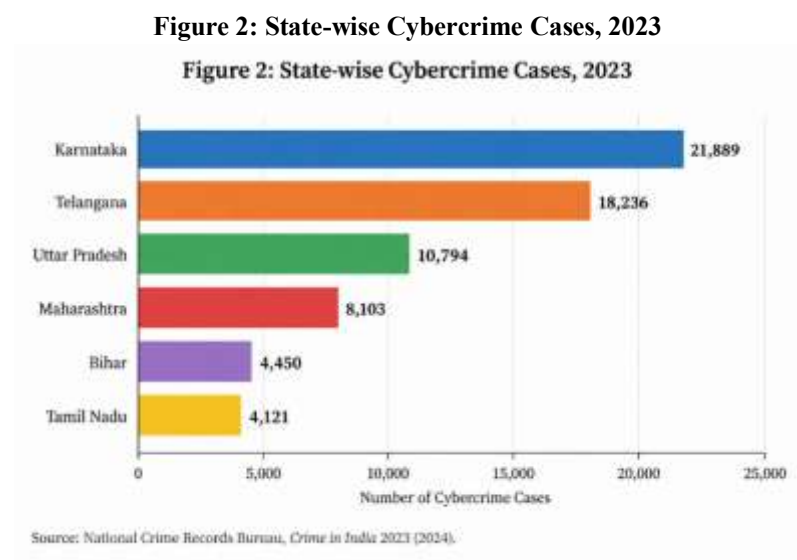
⁷ National Crime Records Bureau, Ministry of Home Affairs, Government of India, *Crime in India 2023*, Vol. I (2025).



State-wise data further demonstrate considerable geographical concentration. Karnataka recorded the highest number of cybercrime cases in 2023 with 21,889 cases, followed by Telangana (18,236), Uttar Pradesh (10,794), Maharashtra (8,103), Bihar (4,450) and Tamil Nadu (4,121). These six States together accounted for approximately 78% of all State-level cases reported in 2023. However, NCRB cautions that States and Union Territories should not be compared solely on absolute crime figures because differences in population, reporting and registration practices may affect the recorded numbers.⁸

Table 3: States with Highest Reported Cybercrime Cases, 2023

Rank	State	Cases
1	Karnataka	21,889
2	Telangana	18,236
3	Uttar Pradesh	10,794
4	Maharashtra	8,103



A particularly important finding for the present research is that the NCRB 2023 dataset separately records cybercrimes against children, including State/UT-wise data. This is significant because children must not be

⁸ National Crime Records Bureau, Ministry of Home Affairs, Government of India, Crime in India 2023, Vol. I (2025).

viewed only as potential offenders in the digital environment; they are also vulnerable victims of cyber-enabled exploitation and abuse. The availability of a separate government dataset on cybercrimes against children provides an important basis for examining the protective dimension of India's juvenile justice system. At the same time, the absence of a comprehensive NCRB category specifically identifying juvenile offenders in cybercrime cases represents an important empirical limitation and research gap.⁹

Table 4: Empirical Significance for Juvenile Justice

NCRB Finding	Relevance to Juvenile Justice
86,420 cybercrime cases in 2023	Expanding digital-crime environment
31.2% increase over 2022	Increasing need for cyber-law preparedness
68.9% cases motivated by fraud	Need for digital and financial literacy
Separate data on cybercrime against children	Children are also victims of digital crime
No comprehensive separate juvenile-offender cybercrime category	Significant data/research gap
Large State-wise variation	Need for State-specific cyber-justice capacity

The NCRB evidence establishes that cybercrime is expanding rapidly in India, but it also reveals a significant limitation for juvenile justice research: national crime statistics do not yet provide a sufficiently detailed picture of children who themselves become involved in cybercrime. The available data nevertheless demonstrate the scale and changing nature of the digital environment in which juvenile offending and victimisation occur. Therefore, India's juvenile justice system requires better age-disaggregated cybercrime data, specialised cyber-investigation capacity, digital literacy programmes and child-sensitive mechanisms for dealing with technology-related offences. The distinction between juvenile cyber offenders and child victims of cybercrime should remain central to future policy so that technological offending is addressed without weakening the rehabilitative and rights-based foundations of juvenile justice.¹⁰

5. Children as Victims of Technology-Facilitated Crimes

The rapid expansion of smartphones, social-media platforms, online gaming, messaging applications and other digital technologies has significantly changed the nature of risks faced by children. Technology has created valuable opportunities for education, communication and social participation, but it has also enabled new forms of victimisation. Children may be subjected to cyberbullying, online grooming, sextortion, identity misuse, privacy violations, sexual exploitation and the circulation of child sexual abuse material ("CSAM"). The characteristics of the digital environment-particularly anonymity, accessibility, speed of dissemination and the ability to reproduce content indefinitely-can increase both the scale and duration of harm. These forms of victimisation require a child-sensitive legal response because the consequences may extend beyond the original incident and affect a child's psychological well-being, dignity, education, family relationships and social development.¹¹

5.1 Cyberbullying and Online Harassment

Cyberbullying involves the use of digital communication technologies to repeatedly intimidate, threaten, humiliate, insult or socially isolate a child. Unlike conventional bullying, cyberbullying may continue beyond school premises and may reach a victim at home through smartphones and social-media applications. Images, videos, comments or messages can be rapidly shared among large groups, increasing the victim's exposure and

⁹ National Crime Records Bureau, Ministry of Home Affairs, Government of India, Crime in India 2023, State/UT-wise Cyber Crimes Against Children During 2023.

¹⁰ National Crime Records Bureau, Ministry of Home Affairs, Government of India, Crime in India 2023, Vol. I-II (2025); Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2 of 2016.

¹¹ Protection of Children from Sexual Offences Act, No. 32 of 2012, page 11-15, India Code (2012); Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, page 14-15, U.N. Doc. CRC/C/GC/25 (2021).

making removal difficult. The possibility of anonymous accounts can further encourage perpetrators to engage in conduct that they might not undertake in face-to-face interactions. For children, repeated online humiliation can affect educational participation, social relationships and emotional well-being. The Committee on the Rights of the Child has recognised that States must take appropriate measures to protect children from violence and abuse occurring through digital technologies while ensuring that such measures respect children's rights.¹²

5.2 Online Grooming and Manipulation

Online grooming represents a particularly serious risk because perpetrators may deliberately establish relationships of trust with children for the purpose of sexual exploitation or abuse. Grooming may occur through social-media platforms, online games, messaging applications or other digital communication channels. A perpetrator may initially present himself or herself as a friend, mentor or peer and gradually obtain personal information, photographs or videos from the child before introducing sexualised communication or threats. The Protection of Children from Sexual Offences Act, 2012 recognises sexual harassment of children and includes conduct involving repeated communication or contact with a child through electronic or digital means for specified sexual purposes. This recognition is important because grooming frequently develops gradually, before physical contact or overt sexual exploitation occurs.¹³

5.3 Sextortion and Sexual Blackmail

Sextortion involves the use of sexually explicit images, videos or other intimate digital material to threaten, intimidate or blackmail a child. In many cases, an offender may first obtain an image through deception, grooming or coercion and subsequently threaten to publish or distribute it unless the child provides additional material, money or performs a particular act. The digital nature of the material enables offenders to threaten distribution to a potentially unlimited audience, creating intense fear and psychological pressure. Where the material concerns a child, the conduct may intersect with several provisions of POCSO and the Information Technology Act, particularly provisions addressing sexual exploitation and material depicting children in sexually explicit conduct.¹⁴

5.4 Identity Misuse and Impersonation

Children may also become victims when their personal information, photographs, usernames, passwords or other identifying information is obtained and misused online. Identity misuse may involve creation of fake social-media profiles, unauthorised access to accounts, impersonation or use of a child's identity for fraudulent or abusive purposes. Children may be particularly vulnerable because they may have limited understanding of privacy settings, account security and the long-term consequences of disclosing personal information. Identity-related victimisation can cause reputational harm and may also expose children to further harassment, stalking or exploitation. The legal framework must therefore recognise that protection of children in the digital environment extends beyond preventing physical or sexual harm and includes safeguarding their personal identity and digital reputation.¹⁵

5.5 Privacy Violations and Unauthorised Use of Children's Data

Children's privacy is particularly important because information disclosed during childhood may remain accessible long after the child has reached adulthood. Digital platforms routinely process information relating to children's identity, preferences, activities, communications and online behaviour. Unauthorised collection, disclosure, profiling or misuse of such information can expose children to exploitation and manipulation. The

¹² Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, page 80-82, U.N. Doc. CRC/C/GC/25 (2021)

¹³ Protection of Children from Sexual Offences Act, No. 32 of 2012, page 11, India Code (2012)

¹⁴ Protection of Children from Sexual Offences Act, No. 32 of 2012, page 11-15, India Code (2012); Information Technology Act, No. 21 of 2000, page 67B, India Code (2000)

¹⁵ Information Technology Act, No. 21 of 2000, page 43, 66C, 66D, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, page 9, India Code (2023)

Digital Personal Data Protection Act, 2023 specifically provides enhanced protection for children's personal data and regulates processing activities involving children. These statutory protections reflect the principle that children require a higher degree of protection in relation to personal information because they may not fully understand the consequences of consenting to digital data practices.¹⁶

5.6 Child Sexual Exploitation Through Digital Platforms

Digital technologies have facilitated new methods of sexually exploiting children, including production, transmission, solicitation and distribution of sexually explicit material involving children. Online platforms may also be used to identify vulnerable children, establish contact, obtain explicit material or facilitate commercial exploitation. The POCSO Act provides a specialised legal framework for protecting children against sexual offences and specifically criminalises the use of children for pornographic purposes. Section 15 further addresses storage or possession of child sexual abuse material in specified circumstances. The Information Technology Act, 2000 also contains specific provisions concerning material depicting children in sexually explicit acts or conduct. The overlapping operation of these statutes demonstrates the seriousness with which Indian law treats digital sexual exploitation of children.¹⁷

5.7 Circulation of Child Sexual Abuse Material (CSAM)

The circulation of CSAM creates particularly severe and continuing harm because digital material can be copied, stored, uploaded and redistributed repeatedly. Even when the original offence has ended, continued circulation may repeatedly victimise the child by allowing new persons to access the material. Indian law therefore criminalises various forms of involvement with material depicting children in sexually explicit acts or conduct. The legal response must, however, extend beyond punishment after circulation has occurred and include mechanisms for rapid identification, reporting, preservation of evidence and removal or restriction of unlawful content. A child-centred approach should also ensure that investigative processes do not unnecessarily reproduce or expose the material, thereby causing secondary victimisation.¹⁸

5.8 Psychological and Social Consequences of Digital Victimisation

Technology-facilitated victimisation can produce consequences that are different in scale and duration from many traditional forms of child victimisation. Harmful content can remain available after the original incident, while repeated notifications, messages, reposting and online discussion can continually remind the victim of the abuse. Children may experience fear, shame, social isolation, loss of confidence and disruption of education or family relationships. The possibility that peers, teachers or family members may encounter the material can further increase the child's vulnerability. Consequently, legal intervention should not be limited to criminal investigation but should incorporate counselling, psychological assistance, confidentiality and rehabilitation consistent with the best interests of the child.

5.9 Children as Both Victims and Participants in Digital Offences

One of the most complex dimensions of technology-facilitated crime is that children may occupy more than one role. A child who initially becomes a victim of grooming, coercion or exploitation may subsequently forward unlawful material, participate in online harassment or become involved in conduct that attracts criminal liability. Such circumstances cannot always be understood through a simple victim-offender distinction. The age of the child, developmental maturity, degree of coercion, influence of adults or peers and circumstances in which the conduct occurred should be carefully considered. The Juvenile Justice (Care and Protection of Children) Act, 2015

¹⁶ Digital Personal Data Protection Act, No. 22 of 2023, page 9, India Code (2023); Committee on the Rights of the Child, General Comment No. 25, page 67-71, U.N. Doc. CRC/C/GC/25 (2021)

¹⁷ Protection of Children from Sexual Offences Act, No. 32 of 2012, page 13-15, India Code (2012); Information Technology Act, No. 21 of 2000, page 67B, India Code (2000)

¹⁸ Information Technology Act, No. 21 of 2000, page 67B, India Code (2000); Protection of Children from Sexual Offences Act, No. 32 of 2012, page 15, India Code (2012); Committee on the Rights of the Child, General Comment No. 25, page 82, U.N. Doc. CRC/C/GC/25 (2021)

is founded upon principles including dignity, participation, best interests, rehabilitation and restoration, which are particularly relevant to children involved in digital offences.¹⁹

5.10 Vulnerability of Children in the Digital Environment

Children's vulnerability to technology-facilitated crimes is influenced not merely by access to technology but also by age, developmental maturity, digital literacy, family environment and awareness of online risks. Younger children may have difficulty identifying manipulation, whereas adolescents may be more willing to engage with strangers or share personal information in online communities. Peer pressure and the desire for social acceptance can also encourage risky online behaviour. Consequently, preventive strategies must move beyond simply restricting children's access to technology and instead promote age-appropriate digital literacy, critical thinking, privacy awareness and knowledge of reporting mechanisms. Such an approach is consistent with the international recognition of children's evolving capacities and their right to participate safely in the digital environment.

5.11 Role of Parents, Schools and Digital Platforms

Protection against technology-facilitated victimisation requires coordinated participation by parents, educational institutions, law-enforcement agencies and online platforms. Parents and teachers can play an important role in identifying behavioural changes, explaining responsible digital practices and encouraging children to report abuse without fear of punishment or stigma. Digital platforms also have responsibilities concerning mechanisms for reporting harmful content, protecting children's accounts and responding appropriately to unlawful activities. However, protective interventions should not become excessive surveillance of children because unrestricted monitoring may itself interfere with privacy and autonomy. The appropriate approach is therefore one that combines safety, education, accountability and respect for children's rights.

5.12 Need for a Child-Centred Legal Response

The increasing victimisation of children through digital technologies demonstrates the need for a comprehensive child-centred response that integrates criminal law, juvenile justice, data protection, cyber-forensics and child-protection mechanisms. Effective protection should include accessible reporting systems, prompt investigation, preservation of digital evidence, removal or restriction of unlawful material, confidentiality of victims and access to psychological and legal support. At the same time, children who become involved in unlawful digital conduct should be assessed within the rehabilitative framework of juvenile justice rather than being treated automatically as adult offenders. The central objective should be to prevent further harm while protecting the child's dignity, privacy, development and long-term interests.

6. Legal Framework Governing Technology-Related Juvenile Delinquency in India

India's legal response to technology-related juvenile delinquency is distributed across several statutes rather than contained in a single comprehensive framework. The Juvenile Justice (Care and Protection of Children) Act, 2015 establishes the principal framework for children alleged to have committed offences and provides mechanisms such as the Juvenile Justice Board, preliminary assessment in specified circumstances and rehabilitative measures. The Information Technology Act, 2000 provides the principal statutory framework for several categories of cyber offences, while the POCSO Act, 2012 specifically addresses sexual offences against children, including conduct that may occur through digital technologies.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 further regulate intermediary responsibilities concerning unlawful information, grievance redressal and cooperation with lawful investigations. The Digital Personal Data Protection Act, 2023 introduces specific safeguards concerning children's personal data, including requirements relating to processing of children's data and restrictions on tracking, behavioural monitoring and targeted advertising directed at children. The interaction between these laws

¹⁹ Juvenile Justice (Care and Protection of Children) Act, No. 2 of 2016, page 3, India Code (2015); Committee on the Rights of the Child, General Comment No. 25, page 18-20, U.N. Doc. CRC/C/GC/25 (2021)

raises important questions concerning overlapping jurisdiction, intermediary responsibility, parental consent, age verification, privacy and the treatment of children who themselves commit cyber offences.²⁰

7. Digital Evidence and Investigation in Juvenile Cybercrime

Digital evidence is central to the investigation of technology-related offences involving juveniles. Social-media conversations, emails, screenshots, photographs, videos, location information, call records, device data and metadata may establish communication, identity, chronology and the circumstances surrounding an alleged offence. However, digital evidence is inherently vulnerable to alteration, deletion, duplication and manipulation. Consequently, investigators must establish its authenticity and reliability through proper collection, preservation and forensic examination rather than relying solely on screenshots or user-generated copies.²¹

The problem becomes more sensitive when the evidence concerns children because investigation may involve accessing highly private communications, mobile devices, photographs or intimate material. A reliable chain of custody, forensic imaging, documentation of seizure and appropriate authentication procedures are therefore essential to protect both the integrity of evidence and the rights of the child. Investigative agencies must simultaneously avoid unnecessary exposure or duplication of sensitive child-related material. The Supreme Court's recognition of privacy as a constitutionally protected right reinforces the need for proportionality and safeguards while collecting and processing digital evidence involving juveniles.²²

8. Juvenile Justice and Human Rights in the Digital Environment

The digital environment requires a careful balance between protecting children from online harm and respecting their fundamental rights. Children are entitled to privacy, dignity, freedom of expression and access to information, while simultaneously requiring protection from exploitation, abuse and harmful digital practices. The principle of the best interests of the child must therefore guide governmental, judicial and institutional responses to juvenile cybercrime. A purely punitive approach may undermine rehabilitation and fail to recognise the developmental characteristics and evolving capacities of adolescents.

The international framework has been strengthened by General Comment No. 25 of the Committee on the Rights of the Child, which recognises that children's rights apply fully in the digital environment and requires States to protect children while respecting their autonomy and evolving capacities. This framework is particularly relevant to juvenile cybercrime because the same child may simultaneously require protection from online exploitation and accountability for unlawful digital conduct. India's juvenile justice response should therefore prioritise proportionality, rehabilitation, privacy and reintegration rather than treating technological misconduct exclusively through a punitive lens.

9. Challenges in Addressing Technology-Related Juvenile Delinquency

Technology-related juvenile delinquency presents distinctive legal, technological and institutional challenges because digital offences can be committed anonymously, across jurisdictions and through rapidly changing technologies. The investigation of such offences becomes more complex when the accused is a child, as authorities must simultaneously ensure effective investigation and uphold the principles of dignity, privacy, best interests and rehabilitation under the juvenile justice framework. The major challenges are discussed below.

9.1 Lack of Cyber-Trained Police Personnel

²⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II, sec. 3(i), extraordinary, G.S.R. 139(E) (Feb. 25, 2021); Digital Personal Data Protection Act, No. 22 of 2023, page 7, 9, India Code (2023)

²¹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, page 61-63, India Code (2023); Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1

²² K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; Bharatiya Sakshya Adhiniyam, No. 47 of 2023, page 61-63, India Code (2023)

The investigation of cyber offences requires specialised knowledge of social-media platforms, digital communications, electronic records, mobile devices and cyber-forensic techniques. However, conventional policing methods may not always be adequate for identifying, collecting and analysing digital evidence. Lack of adequately trained personnel can result in improper seizure of devices, inadequate preservation of electronic records and delays in investigation. In cases involving juveniles, police officers must additionally understand child-sensitive procedures and the requirements of the Juvenile Justice Act. Strengthening specialised cybercrime units and providing continuous training in both cyber-forensics and juvenile justice is therefore essential.²³

9.2 Limited Digital-Forensic Capacity

Digital-forensic capacity remains an important challenge because cybercrime investigations frequently depend upon evidence stored in smartphones, computers, cloud services and other digital devices. The examination of such devices may require specialised tools and trained forensic experts to recover deleted files, analyse metadata and establish the chronology of digital activity. Limited forensic infrastructure and delays in examination may affect the timely completion of investigations and the reliability of evidence presented before the Juvenile Justice Board or court. Proper procedures for forensic acquisition, preservation and examination are therefore necessary to maintain the integrity of electronic evidence.²⁴

9.3 Anonymity and Fake Digital Identities

Anonymity and the use of fake digital identities make attribution of cyber offences particularly difficult. Juveniles may use pseudonyms, temporary accounts, fake profiles or accounts belonging to other persons, while several individuals may have access to the same device or account. Consequently, the registered owner of an account or device cannot automatically be treated as the person responsible for the alleged conduct. Investigators may need to correlate account information, device records, IP-related information, communications and other digital evidence before establishing individual responsibility. This creates significant evidentiary challenges, particularly where the digital identity has been deliberately concealed or manipulated.

9.4 Cross-Border Cyber Offences

The borderless nature of cyberspace creates significant jurisdictional difficulties. A juvenile in India may interact with persons located in another country, use an international digital platform or become involved in an offence where relevant data is stored on servers outside India. Investigators may consequently require information from foreign service providers or assistance from foreign law-enforcement authorities. Differences in legal systems, privacy standards, evidence requirements and procedures for obtaining electronic information can delay investigations. Cross-border cybercrime therefore requires stronger international cooperation and efficient mechanisms for obtaining and authenticating electronic evidence from foreign jurisdictions.

9.5 Difficulties Before Juvenile Justice Boards

Juvenile Justice Boards face a specialised challenge when dealing with technology-related offences because they must evaluate technically complex digital evidence while also considering the child's developmental circumstances. Under the Juvenile Justice Act, the Board is required to follow a child-friendly approach and, in specified cases, undertake a preliminary assessment concerning the child's mental and physical capacity, ability to understand the consequences of the alleged conduct and the circumstances in which the offence was committed. These requirements can become particularly complex where the alleged cyber conduct involves peer influence, online experimentation, grooming, coercion or manipulation. Adequate legal and technological expertise is therefore necessary to ensure that digital evidence is properly understood without compromising the rehabilitative philosophy of juvenile justice.²⁵

²³ Information Technology Act, No. 21 of 2000, page 70B, India Code (2000); Juvenile Justice (Care and Protection of Children) Act, No. 2 of 2016, page 10-14, India Code (2015)

²⁴ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, page 61-63, India Code (2023); Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1

²⁵ Juvenile Justice (Care and Protection of Children) Act, No. 2 of 2016, page 14-18, India Code (2015)

9.6 Inadequate Digital Literacy

Inadequate digital literacy among children, parents, teachers and other stakeholders can contribute both to victimisation and juvenile involvement in cyber offences. Children may not fully understand the consequences of sharing personal information, communicating with strangers, forwarding harmful material or participating in online harassment. Parents and educational institutions may also face difficulties in identifying emerging forms of cyber exploitation and responding appropriately. Lack of awareness may consequently result in delayed reporting and loss of important digital evidence. Digital literacy should therefore include not only technical skills but also awareness of privacy, online safety, responsible digital behaviour and available reporting mechanisms.²⁶

9.7 Platform Cooperation and Evidence Preservation

Social-media companies, messaging services and other online platforms may possess important information relating to cyber offences, including account details, activity records and other relevant electronic information. Investigative agencies may face difficulties in obtaining such information promptly because of platform procedures, jurisdictional issues, data-retention practices or the deletion of accounts and content. Delay in issuing appropriate preservation requests may result in the loss of evidence. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 establish various obligations concerning intermediaries and cooperation with lawful processes, but effective implementation requires timely communication between investigative agencies and platforms. Particular care is necessary where evidence concerns children or sensitive sexual material.

9.8 Balancing Investigation with Children's Privacy

One of the most significant challenges is balancing effective investigation with the child's fundamental right to privacy. A mobile phone or online account may contain extensive personal information unrelated to the alleged offence, including photographs, family communications, educational information and private conversations. Unrestricted examination or disclosure of such information may unnecessarily intrude upon the child's dignity and privacy. The Supreme Court's recognition of privacy as a constitutionally protected right requires State action affecting privacy to satisfy requirements of legality, legitimate purpose, necessity and proportionality. These safeguards are especially important in juvenile proceedings because unnecessary disclosure of personal information may result in stigma and secondary victimisation.

9.9 Overall Assessment

The above challenges demonstrate that technology-related juvenile delinquency cannot be effectively addressed through traditional criminal justice mechanisms alone. Cyber expertise, digital-forensic infrastructure, reliable evidence-preservation mechanisms, international cooperation, digital literacy and child-sensitive adjudication must operate together. At the same time, investigative efficiency cannot override children's rights to privacy, dignity and rehabilitation. India's future response should therefore seek to create a specialised framework in which technological capability and law-enforcement effectiveness are balanced with the fundamental principles of juvenile justice.

10. Legal and Policy Reforms and Conclusion

Legal and policy reform should focus on developing specialised protocols for investigating cyber offences involving children, combined with systematic cyber-safety education and specialised training for police officers, prosecutors and members of Juvenile Justice Boards. Digital evidence procedures should be child-sensitive and should incorporate clear standards for preservation, forensic acquisition, authentication and secure handling of sensitive material. Prevention mechanisms should include accessible reporting systems, awareness programmes for children and parents, and stronger cooperation between government agencies, educational institutions, civil society and online platforms.

²⁶ Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, page32-38, U.N. Doc. CRC/C/GC/25 (2021)

Rehabilitation must remain central where children are found responsible for technology-related offences. Counselling, digital-behaviour education, restorative interventions, skill development and community-based rehabilitation can be more consistent with the objectives of juvenile justice than purely punitive responses. Simultaneously, stronger privacy safeguards and platform accountability are necessary to prevent secondary victimisation and misuse of children's personal information. India's juvenile justice framework must therefore adapt to technological developments while retaining its fundamental child-centred, rehabilitative and rights-based character....

..

.