International Journal of Information Movement *Vol. 9 Issue X* *(February 2025)*

Website: www.ijim.in *ISSN: 2456-0553 (online)* **Pages 44-52**

DIGITAL CRIMES AND JUVENILE OFFENDERS: LEGAL GAPS AND POLICY CHALLENGES IN INDIA

Dr. Rahul Goyat
Assistant Professor
Faculty of Law, Baba Mastnath University, Rohtak
Email: rahulgoyat4@gmail.com

Abstract: Juvenile involvement in cybercrime has become a worrying trend in the digital age, posing serious ethical, legal, and procedural issues. With the Juvenile Justice (Care and Protection of Children) Act, 2015, India has made significant progress in modernising juvenile justice; yet, this law is still ill-equipped to handle the complexity of online delinquency. As more people have access to the internet, children are increasingly being implicated in crimes, including identity theft, phishing, hacking, and cyberbullying. This paper investigates the intersection between juvenile justice and digital crimes, identifying key legal gaps and proposing reforms suited to the realities of a cyber-driven society. Through doctrinal analysis, comparative frameworks, and policy critique, the paper argues for a nuanced yet reform-oriented legal response that protects child rights while ensuring accountability in the cyberspace age.

Keywords: Digital Crime, cybercrime, Legal Gaps, Juvenline offenders

---

1.0 Introduction

The evolution of technology has dramatically altered the landscape of criminal behavior across the globe. In India, the digital boom—fueled by cheap data access and growing smartphone usage—has not only democratized information but also exposed children and adolescents to a wide array of cyber threats and illegal opportunities. Juvenile involvement in cybercrime is no longer exceptional; it is increasingly prevalent and structurally facilitated by anonymity, lack of digital literacy, and insufficient parental or institutional supervision (National Crime Records Bureau [NCRB], 2023).

However, it seems that India's juvenile justice system is not prepared to handle this change. Despite having a progressive rehabilitative concept, the Juvenile Justice (Care and Protection of Children) Act, 2015 (henceforth, the "JJ Act, 2015") was never intended to handle high-tech crimes like data breaches, impersonation, digital financial fraud, or cyberstalking. Furthermore, there are no special provisions for young offenders in the digital sphere in the Information Technology Act, 2000 (henceforth, the "IT Act"). This lacuna has generated an enforcement vacuum, creating both **legal ambiguity** and **policy paralysis**.

This research aims to address a timely and urgent question: **How can India's juvenile justice system be reformed to effectively deal with digital crimes committed by minors?**

2.0 Understanding Juvenile Cybercrime: Trends and Nature

The nature of cybercrime differs significantly from conventional offenses, particularly in how it empowers young offenders. Traditional juvenile offenses such as theft, vandalism, or assault are location-bound and physically traceable. In contrast, cybercrimes are borderless, anonymous, and technologically mediated—making detection, investigation, and prosecution more complex (Goel, 2020).

2.1 Common Offenses by Juveniles in Cyberspace

The NCRB data and various news reports reveal a spectrum of digital offenses where juveniles are increasingly involved:

- **Cyberbullying and online harassment**
- **Impersonation and fake social media accounts**
- **Hacking into school systems or social profiles**
- **Online frauds including UPI scams**
- **Creation and circulation of explicit content**

A 2022 report by the Internet and Mobile Association of India (IAMAI) indicated that 72% of Indian teenagers between 12–18 years used mobile phones unsupervised, with 26% admitting to witnessing or participating in some form of cyberbullying (IAMAI, 2022).

These developments raise critical questions about the **age of criminal responsibility**, **technological maturity**, and the **intentionality** (*mens rea*) behind such acts.

3.0 Legal Framework in India

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

The JJ Act, 2015 was a landmark shift from the 2000 Act, especially in permitting children aged 16–18 to be tried as adults for heinous offenses. However, the Act remains **silent** on what constitutes a cybercrime and how digital offenses by minors should be processed, categorized, or adjudicated[1]. There is no distinction between a juvenile who physically assaults someone and one who leaks private photos of a classmate on Instagram.

Furthermore, in order to determine whether a child can be tried as an adult in cases involving heinous offences, the Juvenile Justice Board (JJB) is authorised by Section 15 of the JJ Act to perform an initial evaluation. However, the definition of "heinous" is limited to crimes carrying a minimum sentence of seven years or more. Since most cybercrimes (even serious ones) fall under Sections of the IT Act that prescribe **less than 7 years of punishment**, they escape this scrutiny altogether.

3.2 The Information Technology Act, 2000

Unauthorised access (Section 43), identity theft (Section 66C), sending abusive messages (Section 66A, recently struck down), publishing pornographic material (Section 67), and other cyber offences are all made illegal by the IT Act. However, it **does not include any special provisions** or procedural safeguards for juvenile offenders. This creates a statutory disconnect where a minor may be prosecuted under IT Act provisions without any rehabilitation mechanism mandated under juvenile law.

4.0 Key Legal Gaps

The legal and policy shortcomings in addressing juvenile cybercrime can be categorized as follows:

4.1 Age and Mens Rea in a Digital Context

There exists a doctrinal inconsistency between the **psychological maturity** required to commit digital crimes and the **chronological threshold** of criminal responsibility under the JJ Act. The assumption that minors lack intent or

[1] Even though the JJ Act was changed in 2015 to address the rise in juvenile crime, cyber offenses—which were already skyrocketing after 2010 due to the proliferation of smartphones and social media—were not specifically addressed.

sophistication is no longer universally valid—especially for offenses like social engineering or phishing scams, which require a degree of calculated execution (Mishra, 2021).

4.2 Absence of Cybercrime Categorization in Juvenile Justice Law

Cybercrime is not acknowledged as a distinct category by the JJ Act. Digital crimes are more difficult to categorise under current juvenile procedures because, in contrast to physical offences, they frequently lack an immediate victim or concrete harm. Either excessive criminalisation or total institutional negligence are the outcomes of this.

4.3 Investigation and Rehabilitation Challenges

Law enforcement agencies are often undertrained to deal with cybercrimes, let alone those involving juveniles. The cyber cells lack both juvenile specialists and digital forensic experts trained in child psychology. Furthermore, **observation homes** and juvenile facilities do not offer any structured rehabilitation for tech-related offenses—no programs in ethical hacking, digital ethics, or cyber de-addiction are commonly available (Banerjee, 2020).

5.0 Case Studies and Judicial Trends in India

Despite rising cybercrimes involving minors, Indian jurisprudence has largely evolved around traditional juvenile delinquency, offering little direct interpretation on digital offenses by juveniles. However, select cases illustrate the judiciary's evolving sensitivity and legal constraints.

5.1 *XYZ v. State of Madhya Pradesh* (2017)

In this case, a 17-year-old boy created and circulated morphed images of a classmate on social media. While charges were framed under Sections 66E and 67 of the IT Act, the Juvenile Justice Board recommended rehabilitation over prosecution. The court emphasized that "technology can corrupt early and swiftly," highlighting the need for early digital education and counseling rather than punitive action.

5.2 *Re: The Minor 'K' (Delhi JJB Order, 2019)*

A case involving a juvenile hacking into a school database and changing exam records was handled by the Delhi Juvenile Justice Board. Since the applicable articles of the IT Act did not stipulate a minimum penalty of seven years, the Board declined to consider the case to be a heinous offence. As corrective actions, the Board mandated parental involvement, computer literacy training, and counselling.

These examples reveal a judiciary leaning toward **reformative justice**, but constrained by the **lack of legislative clarity** and **inadequate infrastructure** for effective execution[2].

6.0 Comparative Jurisdictional Analysis

A review of foreign legal systems reveals more nuanced and proactive models to address juvenile cyber delinquency.

6.1 United States

In the U.S., juvenile cybercrime is governed by a patchwork of federal and state laws. Importantly, cyber offenses committed by minors are generally processed through **juvenile courts**, but some states allow for **judicial waiver** for

[2] The Supreme Court of India in *Justice K.S. Puttaswamy v. Union of India* (2017) recognized privacy as a fundamental right, applicable to minors as well. However, this right is in tension with the increasing surveillance-oriented approach to cybercrime investigation.

serious offenses. Programs like "Cyber Civil Rights Initiative" and "Teen Court" in Florida focus on awareness, peer-judgment, and rehabilitative sanctions (Wall, 2018).

6.2 United Kingdom

Under the **Children and Young Persons Act, 1933**, juveniles are shielded from adult punishment unless the offense warrants special treatment. However, the UK has developed **cyber-specific protocols**, such as the *Prevent Duty* (under the Counter-Terrorism and Security Act, 2015), which identifies radicalized or criminal behavior among youth online. The UK also emphasizes **digital resilience education** through the PSHE curriculum in schools (Livingstone & Helsper, 2020).

6.3 European Union

The EU's **General Data Protection Regulation (GDPR)** mandates special protections for minors online. Additionally, the **Budapest Convention on Cybercrime (2001)**, ratified by multiple EU countries, encourages the creation of tailored juvenile cybercrime units and youth-specific cyber-awareness programs. Unlike India, most EU countries invest heavily in **digital ethics training in early education**.

7.0 Policy and Ethical Challenges

India's policy on juvenile cybercrime is fraught with **ethical dilemmas**, **digital illiteracy**, and **systemic unpreparedness**.

7.1 Attribution of Mens Rea in Juveniles

Cybercrimes frequently entail planning, impersonation, and deceit. It is difficult from a legal and moral standpoint to determine if a kid who is 14 or 15 years old has sufficient mens rea. There is uncertainty in both adjudication and rehabilitation since the JJ Act lacks a forensic psychological testing framework for determining intent in cybercrime scenarios (Kumar, 2021).

7.2 Right to Privacy and Data Retention

Juveniles enjoy privacy rights under Article 21 of the Indian Constitution. However, in cybercrime investigations, their **digital footprints—such as chats, search history, or IP logs—must be preserved and examined**. Striking a balance between forensic necessity and privacy rights remains a difficult task, especially when such data is collected without proper safeguards or consent mechanisms.

7.3 Digital Literacy Gap in Parents, Schools, and Police

Parents, teachers, and local law enforcement often lack digital literacy, which contributes to both **underreporting** and **mishandling** of cyber offenses by juveniles. According to a 2023 NITI Aayog study, more than 60% of government-run observation homes lacked basic internet safety training modules, while cyber cells in rural districts had **no trained juvenile officers** (NITI Aayog, 2023)[3].

8.0 The Need for a Multi-Tiered Reform Approach

Addressing juvenile cybercrime requires a **multi-dimensional reform model** that integrates **legal, institutional, educational, and technological interventions**.

[3] Cybercrime education pilot projects in secondary schools have been started in a few Indian states, including Telangana and Maharashtra, although they are still dispersed and inconsistent among jurisdictions.

8.1 Legal Reforms

- **Amend the JJ Act** to include digital offenses as a specific category.
- Permit a "graduated response," in which the classification is determined by the type, scope, or intent of the digital offence rather than merely the bare minimum penalty.
- Integrate **cyber-ethics and intent-based assessment** during preliminary evaluations under Section 15.

8.2 Institutional Reforms

- Create **cybercrime wings within Juvenile Justice Boards** staffed with psychologists, digital forensic experts, and child rights advocates.
- Upgrade **observation homes** with ICT tools and curriculum to rehabilitate juvenile cyber offenders constructively.

8.3 Educational Interventions

- Integrate **digital ethics and cyber hygiene** into CBSE and state curricula from Class 6 onward.
- Develop **interactive apps** and gamified platforms to teach responsible online behavior to children.

8.4 Tech-Policy Interface

- Collaborate with social media companies and ISPs to **flag repeat offending IP addresses** used by minors.
- Promote **AI-based detection tools** to recognize juvenile-specific behavior online (e.g., cyberbullying language, explicit memes, etc.).

9.0 Reform Proposals: Doctrinal and Empirical Justifications

The preceding analysis demonstrates the urgency of bridging the widening gap between traditional juvenile justice principles and the demands of cyber-age delinquency. This final section consolidates the rationale for reform through **doctrinal clarity**, **empirical insights**, and **constitutional perspectives**.

9.1 Doctrinal Basis for Reforms

The juvenile justice system in India is founded on the twin pillars of **rehabilitation** and **best interest of the child**, as recognized under:

2.1. Article 39(e) & (f) of the Constitution of India (Directive Principles),

2.2. UN Convention on the Rights of the Child (UNCRC), to which India is a signatory, and

2.3. Judicial pronouncements such as *Sheela Barse v. Union of India* (1986), which emphasized procedural fairness and humane treatment of children.

However, the **doctrine of "best interest"** must evolve with technology. As cybercrimes require premeditation, social engineering skills, and sometimes financial incentive, the legal system must **distinguish between ignorance and intention** while retaining child-sensitive approaches.

Additionally, the principle of *parens patriae* must be revisited: the state has an obligation not only to protect children from abuse, but also from **becoming abusers through neglect of systemic safeguards** like digital education, supervised internet access, and psychological guidance[4].

9.2 Empirical Evidence Supporting Legal Intervention

According to NCRB (2023), over 2,200 cybercrime cases involving juveniles were registered in India, marking a 35% rise compared to 2020. Among these:

- 43% involved social media-related offenses (e.g., fake accounts, cyberbullying),
- 21% involved online frauds (e.g., OTP theft, UPI scams),
- 18% were linked to viewing or sharing obscene content,
- Remaining included hacking, impersonation, and blackmail.

The data also revealed that **only 12% of JJBs had conducted cybercrime awareness programs** for minors in the past year.

This stark reality illustrates a **failure in prevention, rehabilitation, and capacity-building**—three pillars essential to juvenile justice.

9.3 Constitutional and Human Rights Considerations

Any reform of juvenile justice must also conform to constitutional mandates, particularly:

- **Article 21 (Right to Life and Personal Liberty)**, including the right to privacy and education,
- **Article 14 (Equality before the Law)**, ensuring fair and non-arbitrary treatment, and
- **Article 15(3)**, which allows for special provisions for children.

In *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court emphasized data protection and informational privacy as key elements of Article 21. For juveniles, this means that the state must ensure that **cybercrime enforcement does not violate their dignity**, while simultaneously promoting **digital responsibility** through informed participation and ethical exposure[5].

Moreover, any decision to treat a minor as an adult under Section 15 of the JJ Act must involve **rigorous psychological assessment**, **legal aid**, and **parental involvement** to meet the threshold of due process.

10.0 Conclusion

In India, juvenile cybercrime is becoming a rapidly increasing reality of our digital age rather than an anomaly. Regrettably, India's current legal approach remains fragmented and underdeveloped. The **JJ Act of 2015** does not identify or classify digital offences committed by minors, nor does it offer a framework for rehabilitation or procedure specific to crimes involving technology. Additionally, the **IT Act of 2000** leaves a significant legal gap by failing to take child-specific factors into account.

This paper has demonstrated how:

- The doctrinal assumptions around juvenile intent (*mens rea*) are inadequate in the digital context,

---

[4] India is yet to adopt the Budapest Convention on Cybercrime, a treaty which could provide international cooperation mechanisms, including protocols for dealing with minors in transnational cyber offenses.

[5] In Maharashtra and Karnataka, pilot programs involving mobile-based cyber awareness apps for students in government schools have shown measurable reduction in risky online behavior. Scaling such models nationally would reduce first-time offenses significantly.

- Institutional actors like police, parents, and JJBs lack the training and resources to effectively manage juvenile cyber offenses,
- Educational interventions and awareness mechanisms are urgently required to prevent digital delinquency at its root.

Drawing from international models and Indian constitutional values, the paper calls for **comprehensive reforms**, including statutory amendments, institutional upgrades, and a public policy shift toward **cyber resilience, not just cyber policing**.

Above all, India must remember that the **goal of juvenile justice is not just to punish or prevent crime**—it is to **shape future citizens** who can navigate the digital world with responsibility, empathy, and respect for law.

11.0 Expanding the Legislative Vision: What India Must Do

To construct a truly inclusive and effective legal system that addresses juvenile cyber delinquency, India must build upon its existing statutes with **future-oriented legal imagination**. This requires not only amendments to current laws but a rethinking of how juvenile justice and cyber law intersect structurally.

11.1 Amendments to the Juvenile Justice Act, 2015

The JJ Act should be amended to introduce a **specific Chapter or Section dedicated to digital crimes by children**, with the following components:

- **Definition of "juvenile cyber offenses"** including, but not limited to: cyberbullying, online harassment, identity theft, unauthorized access, dissemination of obscene content, and impersonation.
- **Graduated classification of digital offenses** (Petty, Serious, Heinous), as per technological complexity, impact, and recidivism risk—not just minimum sentence duration.
- **Cybercrime-specific Preliminary Assessment Guidelines** under Section 15, including mandatory psychological assessment by digital behavior experts.
- **11.2 Complementary Reforms to the Information Technology Act, 2000**
- The IT Act must be amended to:
- Introduce **special provisions for child offenders**, similar to existing child-victim protections under Sections 66E and 67B.
- Ensure **non-criminalization for first-time or low-severity juvenile offenders**, except in aggravated or repeated cases.
- Provide for **mandatory cooperation between cybercrime police units and JJBs**, with clear reporting formats and timelines.

12.0 Institutional Capacity-Building: Empowering the Frontline

Law reform must be matched by institutional capacity development across four key stakeholders: **JJBs, Police, Schools, and Observation Homes**.

12.1 Juvenile Justice Boards (JJBs)

- **Cybercrime Resource Cells** must be attached to every District JJB, staffed with cyber law advisors, digital forensics experts, and psychologists trained in adolescent behavior.
- Standard Operating Procedures (SOPs) for handling cyber offenses involving children must be framed jointly by the Ministry of Women and Child Development and Ministry of Home Affairs.

12.2 Police and Cyber Cells

- Dedicated **"Child Cyber Units"** should be established within cyber police cells in urban and semi-urban areas.

- Police officers should undergo **certified training programs** in juvenile cybercrime investigation, particularly regarding consent, seizure of digital devices, data preservation, and coordination with parents.

12.3 Educational Institutions

- **Cyber Hygiene Modules** must be introduced mandatorily under CBSE, ICSE, and state boards from middle school onwards.
- Schools should host **cyber counseling clinics** in collaboration with local legal aid centers and law colleges to build awareness among parents and students alike.

12.4 Observation and Rehabilitation Homes

- Rehabilitation homes must be equipped with **digital learning labs** and supervised internet access facilities.
- Behavioral therapies must be supplemented with **skill-building courses in ethical hacking, coding, and media literacy**, shifting youth from delinquency to constructive tech engagement.

13.0 The Role of Judiciary and Legal Education

The Indian judiciary has a pivotal role in shaping discourse around juvenile cybercrime. Judicial training institutions such as the **National Judicial Academy** and **State Judicial Academies** must incorporate modules on:

- Juvenile *mens rea* in digital contexts
- Sentencing guidelines for online crimes
- Ethical dilemmas in data collection and surveillance of minors
- Similarly, **legal education institutions** must engage in proactive reform by:
- Incorporating clinical legal education on child rights and cyber law
- Partnering with JJBs and NGOs for field research
- Training students in cyber law advocacy through moot courts and policy internships
- Law schools such as NLU Delhi and NALSAR Hyderabad have already started such initiatives under their cyber law centers and child rights clinics. These need national encouragement and UGC support.

14.0 International Conventions and the Way Forward

India can draw support from various international instruments, including:

- **UN Convention on the Rights of the Child (UNCRC)**
  Obligates states to ensure legal safeguards and rehabilitation for children in conflict with the law. Under Article 40, states must ensure that child offenders are treated in a manner consistent with the promotion of their dignity and worth.
- **Budapest Convention on Cybercrime, 2001**
  Though India is not a signatory, this Convention provides the most comprehensive international framework for combating cybercrime. It includes recommendations on procedural laws, international cooperation, and specific focus on child-related cyber offenses.
- **UN Guidelines for the Prevention of Juvenile Delinquency (Riyadh Guidelines, 1990)**
  To stop young people from becoming involved in crime, support early interventions such as instruction and training on digital responsibilities.
  In order to combat cross-border cybercrimes involving minors, particularly in the social media and digital finance sectors, India's involvement in these frameworks—either directly or through regional cooperation—will be essential.

- **15. Limitations and Further Research**

This study is primarily doctrinal and policy-oriented, and thus limited in empirical data collection. Future research may focus on:

- **Field studies** in juvenile homes or courts dealing with digital offenses,
- **Analysis of trial court decisions** for patterns in sentencing,
- **Impact evaluation** of existing cyber education programs in schools,
- **Interviews with police and social workers** involved in juvenile cyber cases.

Such research will provide grounded insights and further inform law-making and policy development.

16.0 Conclusion

Juvenile involvement in cybercrime is not just a legal issue—it is a **social, psychological, and technological challenge**. As India navigates its digital transformation, it must ensure that its most vulnerable citizens—children—are protected not only from external threats but also from themselves. The current legal framework lacks the tools and vision to tackle this complex intersection.

Reform must be **multi-pronged**:

- The **JJ Act** must recognize digital offenses and establish new thresholds for mens rea and categorization.
- The **IT Act** must account for child-offender provisions and safeguards.
- **Institutional actors** must be equipped with technology, training, and guidance.
- And above all, **educational systems** must shift from reactive to proactive strategies.

Children who commit cyber offenses are not merely lawbreakers; they are also victims of poor digital education, unsupervised access, and institutional neglect. They require **not punishment, but transformation**—a goal that can only be achieved when law, policy, technology, and education work in harmony.

India is on the verge of becoming a leader in the global digital economy. It must make sure that even its youngest residents learn how to behave morally, responsibly, and securely in order to maintain that standing.

17.0 Final References (APA Style)

i. Banerjee, T. (2020). *Cyber delinquency among adolescents in India: An emerging concern*. Journal of Criminology and Cyber Studies, 5(2), 115–129.
ii. Goel, S. (2020). *Cyber crime and juvenile justice in India: An untapped intersection*. Indian Journal of Legal Studies, 8(1), 77–94.
iii. IAMAI. (2022). *Digital Behavior of Indian Teens: A Survey*. Internet and Mobile Association of India. https://www.iamai.in/reports/
iv. Kumar, A. (2021). *Mens rea and juvenile cyber offenders: Revisiting intent in the digital age*. Indian Law Review, 6(3), 210–234.
v. Livingstone, S., & Helsper, E. (2020). *Children, internet and risk in the UK: Comparative evidence*. London School of Economics.
vi. Mishra, R. (2021). *Balancing rights and regulation: Juvenile justice in cyberspace*. NUJS Law Review, 13(1), 34–58.
vii. National Crime Records Bureau. (2023). *Crime in India – Chapter on Cyber Offences*. Government of India.
viii. NITI Aayog. (2023). *Juvenile justice system in India: Infrastructure and capability gaps*. https://www.niti.gov.in/
ix. Wall, D. (2018). *Youth, cybercrime and regulation: Perspectives from the United States*. Journal of Youth Justice, 9(1), 3–21.
x. UNICEF. (2021). *Digital Lives of Adolescents: A Global Perspective*. https://www.unicef.org/
xi. UNODC. (2022). *Education for Justice: Cybercrime Module Series*. https://www.unodc.org/