Scholarly Research Journal for Interdisciplinary Studies
Online ISSN 2278-8808, SJIF 2026 = 8.727
https://www.srjis.com/issues_data/290
Peer Reviewed & Refereed Journal, MAR-APRIL 2026, Vol- 14/94

ADDRESSING JUVENILE CYBERCRIME: IDENTIFYING LACUNAE IN THE JUVENILE JUSTICE (CARE AND PROTECTION OF CHILDREN) ACT, 2015

Brahmacharimayum Debajit Sharma
Research Scholar, Department of Law, School of Legal Studies, Dhanamanjuri University, Imphal, India
Dr. Yumkham Sarojbala
Assistant Professor, Department of Law, School of Legal Studies, Dhanamanjuri University, Imphal, India
Dr. Yailiwon Shangh
Assistant Professor, Department of Law, School of Legal Studies, Dhanamanjuri University, Imphal, India

Paper Received On: 20 MAR 2026
Peer Reviewed On: 24 APRIL 2026
Published On: 01 MAY 2026

Abstract

The rapid growth of digital technology has transformed the nature of juvenile delinquency, with children increasingly engaging in cyber-related offences such as hacking, identity theft, cyberbullying, and online fraud. This article examines the lacunae within the Juvenile Justice (Care and Protection of Children) Act, 2015 in addressing cybercrime committed by children in conflict with law. The primary objective of the study is to analyse the inadequacy of the existing punishment-based classification of offences under the Act and its inability to effectively respond to the complexities of cyber delinquency. The research adopts a doctrinal and analytical methodology through the examination of statutory provisions, case-related literature, journal articles, and comparative international practices. The study finds that the absence of cyber-specific provisions, inadequate rehabilitation mechanisms, and lack of institutional preparedness create significant gaps in the juvenile justice framework. It further argues for impact-based classification of cyber offences, inclusion of specialised procedural safeguards, and development of technology-oriented rehabilitation measures to ensure a balanced and child-centric approach in the digital era.

Keywords: *Cyber Delinquency, Child in Conflict with Law, Juvenile Justice Act, 2015, Cybercrime, Rehabilitation and Reformative Justice*

1. Introduction

The emergence of digital technologies has fundamentally altered the landscape of criminal activity, including offences committed by children. Children are now able to participate in activities that may be considered cyber offenses due to the increased availability of internet access, smartphones, social media platforms, and anonymous feature, often without fully understanding their legal consequences. When a child lacks the capacity to understand the legal consequences of their actions, the principle applied is *doli incapax* which is a Latin phrase meaning "*incapable of doing harm*" or "*incapable of committing a crime*". It is a doctrine in criminal law which presumes that a child below a specified age does not possess the mental capacity, or *mens rea* (guilty mind), to comprehend the nature, wrongfulness, or consequences of their actions. It is a tenet of criminal law holding that a kid under a certain age does not have the ability to reason.

This shift from the traditional to the digital era necessitates a re-examination of existing juvenile justice frameworks to determine their adequacy in addressing such evolving forms of delinquency. In India, children in conflict with law are governed by the Juvenile Justice (Care and Protection of Children) Act, 2015 (hereinafter JJ Act). Despite the Act being based on the ideas of rehabilitation and reform, it classifies offences into petty, serious, and heinous categories based on the severity of punishment prescribed under substantive criminal law. However, this classification appears inadequate in the context of cybercrime, where the harm caused may be significant and harsh when compared to statutory punishments which is relatively lower. This paper contends that there is a significant gap in the JJ Act to effectively address cyber delinquency. It seeks to examine the implications of this gap and proposes reforms to align the law with contemporary technological realities. Furthermore, it incorporates a brief comparative analysis to address cyber offences involving children in conflict with law and their rehabilitation.

2. Concept of Child in Conflict with Law

The JJ Act classifies children into two categorises viz., “child in need of care and protection” & “child in conflict with law”. A “child in conflict with law” is defined as a person alleged or found to have committed an offence while below the age of eighteen years. The Act is founded on the principle that children are capable of reformation and therefore, should not be subjected to the same punishment procedures as adults. Rehabilitation, social reintegration, and the child's best interests are the main focus of India's juvenile justice

system. Institutions such as State Child Protection Society, Juvenile Justice Boards, State Child Protection Units, District Child Protection Units are tasked with ensuring that children are dealt with in a child-friendly manner, focusing on correction rather than punishment. However, the introduction of the "heinous offence" category in the JJ Act, 2015 marked a shift towards a more punitive approach in certain cases, allowing children aged 16-18 years to be tried as adults for grave crimes. The adequacy of the classification scheme is called into question by this advancement, especially in the case of cybercrime.

3. Classification of Offences under the JJ Act

The JJ Act classifies offences into three categories:

a) Petty offences (Section 2(45)): Punishable with imprisonment up to three years.

b) Serious offences (Section 2(54)): Punishable with imprisonment between three to seven years. [However, with the advent of the Juvenile Justice (Care and Protection of Children) Amendment Act, 2021, it has classified offenses as "serious offences" which have a maximum sentence of 7+ years but either have no minimum penalty or have a minimum penalty of fewer than 7 years."]

c) Heinous offences (Section 2(33)): Offences for which the minimum punishment is seven years or more.

This classification is based entirely on the quantum of punishment prescribed under substantive laws such as the Bharatiya Nyaya Sanhita, 2023 (which replaced the Indian Penal Code, 1860) and the Information Technology Act, 2000, (hereinafter IT Act) and has significant procedural implications. For instance, in cases involving heinous offences, a preliminary assessment is conducted to determine whether a child aged 16-18 years should be tried as an adult. Consequently, the categorization of offences becomes crucial in determining the trajectory of the case. However, the reliance on punishment as the sole criterion for classification fails to account for the nature, impact, and complexity of modern offences, particularly cybercrimes. This is problematic because it overlooks the actual nature and consequences of modern crimes, especially cybercrimes. Unlike traditional offences, cybercrimes may result in extensive and enduring harm such as financial losses affecting multiple victims, reputational harm, or severe psychological distress, despite attracting comparatively lighter statutory penalties under the IT Act. For instance, a single act of data breach or online exploitation by a juvenile can impact hundreds or even thousands of individuals, rendering its consequences far more severe than what the prescribed punishment

suggests. By concentrating just on the length of the incarceration, as opposed to the real harm, scale, and technological complexity, the law fails to adequately capture the seriousness of the offence. As a result, significant cybercrimes are mistakenly labelled as "non-heinous," or “less serious” which restricts the scope of appropriate legal action and tailored rehabilitation measures.

4. Nature and Scope of Cybercrime by Children

Cybercrime encompasses a wide range of illegal acts committed using digital methods. The COVID-19 pandemic is particularly relevant here, as it resulted in a significant reliance on digital platforms which included the educational and the juvenile social interactions. Common forms of cyber offences committed by juveniles include:

I. Unauthorized access and hacking
II. Identity theft
III. Online harassment and cyberbullying
IV. Financial fraud
V. Circulation of obscene or illegal content

The IT Act provides the principle legal framework for addressing cyber offences in India. However, since most offences under this Act carries penalties of less than seven years, they fall outside the “heinous offence” classification under the JJ Act. The unique characteristics of cybercrime make it particularly challenging, which includes the following-

- Transnational scope: Offences may involve victims across jurisdictions
- Anonymity: Perpetrators/Offenders have the ability to hide their identities.
- Scale of harm: A single act can affect thousands of victims
- Psychological impact: Victims may suffer long-term emotional damage

Despite these factors, the legal system often treats such offences as less serious due to the lower statutory punishment attached with them. However, in reality, cybercrime is extremely serious, posing major threats not only to individuals but to businesses and even national security. It causes billions in financial losses, leads to identity theft, ruins reputations, and can cripple critical infrastructure. With rising threats like ransomware and phishing, it is a top-tier security risk worldwide.

5. The Existing Legislative Deficiency in the JJ Act

The central lacuna in the JJ Act lies in its failure to properly classify and address cyber offences committed by children. It has also failed to define cyber delinquency, digital violence, virtual harm, AI-assisted juvenile offences This gap arises primarily from the punishment-based classification system, which can be discussed under the following heads-

5.1 Punishment v. Impact

The Act equates the seriousness of an offence with the length of punishment prescribed. However, in the context of cybercrime, the impact of an offence may be severe even if the prescribed punishment is relatively low. For example, a juvenile involved in a large-scale online fraud or the dissemination of explicit content may cause significant harm, yet the offence may not qualify as "heinous" under the Act.

5.2 Misclassification of Cyber Offences

Since most cyber offences carry a punishment of less than seven years, they are categorized as "non heinous" or "less serious" within the prevailing structure of the JJ Act. This poses several challenges that can be discussed as follows-

- Inadequate legal response- the absence of a "cyber delinquency category" in the JJ Act results in misclassification of offences affecting children in conflict with law. As a result, the legal response may fail to reflect the technological complexity and possible harm of such crimes.
- Lack of appropriate intervention mechanisms- Authorities dealing with juveniles involved in cybercrime often lack digital literacy and technical expertise. These hampers understanding the nature of cyber offences accurately and designing suitable rehabilitative measures.
- Underestimation of the gravity of offences- Since cyber offences such as identity theft, online harassment, hacking, etc., are not tangible in nature, they are not well known. Therefore, such crimes may fail to attract sufficient attention to their psychological, financial, and societal impact.

5.3 Absence of Cyber-Specific Provisions

The JJ Act does not contain any provisions specifically addressing cybercrime. No instructions are provided regarding:

- Procedures in evidence handling- The IT Act (read with general criminal procedure) allows technical methods like device seizure, acquiring and analysing digital evidence.

However, the JJ Act does not lay down child-specific procedures for such actions. This creates confusion on how to legally seize a minor's phone or access their private data while respecting juvenile safeguards.

- Privacy v. investigation conflict- Juveniles are entitled to enhanced privacy and dignity under the Juvenile Justice framework which is clearly mandated under the Act. But cyber investigations often require accessing chats, emails, browsing history, etc. There is no clear rule balancing a child's right to privacy with investigative needs, leading to arbitrary practices.
- Lack of guidelines on admissibility of digital evidence involving minors- While digital evidence is generally governed by rules like electronic records certification (e.g., Section 65B of the Evidence Act, 1872 now covered under section 63 of Bharatiya Sakshya Adhiniyam, 2023), the JJ Act does not clarify how such evidence should be handled when the accused is a child especially in informal or inquiry-based proceedings before the Juvenile Justice Board.

6. Practical Ramifications of the Gap

The IT Act explicitly define cyber offences like hacking, identity theft, fraud, however, due deliberation regarding juvenile offenders were not done when the law was created. Therefore, where juveniles are involved, the Act lacks clarity in prioritising rehabilitation intended under the JJ Act or deterrence along with sanctions proposed in the IT Act. These challenges can be discussed under the following heads:

6.1 Ineffective Deterrence

The law's deterrent effect is weakened when major cyber crimes are treated as non-heinous or less serious and the juveniles may not fully appreciate the seriousness of their actions. Online financial fraud committed by minors, such as phishing or UPI scams, serves as a prime illustration. Suppose a 17-year-old creates a fake banking website and tricks multiple users into sharing OTPs, resulting in substantial financial loss to victims. Under the IT Act, such conduct may be punishable under provisions like identity theft or cheating by personation, but these offences generally carry penalty of less than seven years of imprisonment. Consequently, under the JJ Act, it would not be classified as a "heinous offence," even though the harm caused is significant and involves planning, technical skill, and intent.

6.2 Inadequate Rehabilitation

Presently, rehabilitation programs that exist for CCLs who are alleged or found to have committed a cyber offence are inadequate in observation homes, places of safety, or special homes. Traditional reformative measures may not address the underlying issues, such as:

- Digital addiction
- Neglect of digital responsibility/ethics
- Abuse of IT capabilities

6.3 Challenges for Law Enforcement

Investigating cyber offences requires technical expertise and coordination with cyber cells. The lack of integration between juvenile justice mechanisms and cybercrime units hampers effective enforcement. Cybercrime investigation requires trained digital forensic experts. The IT Act framework assumes such expertise, but the Juvenile Justice system lacks institutional capacity (trained officers, child psychologists & cyber experts), resulting in inconsistent investigation quality.

6.4 Probability of Recidivism

Without targeted intervention, children involved in cybercrime are at a high risk of reoffending, as their actions often go uncorrected at the behavioural and cognitive level. If a juvenile participates in actions like hacking, internet fraud, or cyberbullying without sufficient counselling or digital ethics training, or supervision, they may begin to view such conduct as acceptable or low-risk. Although the JJ Act places a strong emphasis on rehabilitation, this goal is still not fully achieved due to a lack of specialized programs that address digital conduct. Furthermore, the anonymity and technological complexity of cybercrime might lead to a mistaken perception of impunity, which may entice young people to try new things and escalate their conduct. Peer influence, online communities, and easy access to hacking tools can reinforce such behaviour, turning isolated incidents into habitual conduct.

7. Comparative Perspective

As demonstrated by a short comparative study, the problem is not specific to India; instead, the difference is that other nations have begun to modify their legal systems and implement initiatives and processes to fight juvenile cybercrime and rehabilitate the offenders engaged. They make a deliberate effort to incorporate technology into the Juvenile laws, aiming for a balance between rehabilitation and prevention.

It is worthwhile to mention the TRIANGLE Project which is a European initiative focused on improving digital literacy and vocational skills of young people in detention or secure care institutions. It aims to create a secure digital learning platform for juveniles deprived of liberty. The project is implemented in European countries, mainly Netherlands, Belgium and Portugal. It is funded under European cooperation programmes (like Erasmus+). The project aims to-

- Promote digital inclusion in detention centres
- Develop safe online learning environments
- Improve employment opportunities and reintegration after release
- Reduce recidivism by engaging juveniles in structured digital education.

With the objectives in view, the platform provides the following-

- Controlled internet access (whitelisted/filtered)
- Digital literacy education
- Hands-on career preparation
- Instruments for education and rehabilitation

As a result, the initiative is based on three key components namely people, platform, and program with the goal of integrating them to create a supplementary learning environment on a digital platform to improve young people's job prospects upon release from institutions and support their seamless reintegration into society.

The juvenile justice system in the United Kingdom prioritizes rehabilitation, wellbeing, and avoiding the formal criminal justice system wherever possible. The UK laws and international treaties such as the UNCRC require that children be imprisoned only when there are no other options. The UK has specialized law enforcement units and organizations (such as the Joint Operations Cell, which combines the National Crime Agency and GCHQ) to address online child sexual exploitation and crimes committed on the dark web. Data security (such as under the GDPR), privacy restrictions, content moderation laws, and platform responsibility all work together to minimize risk and hold perpetrators accountable for online misconduct. Even if juvenile justice laws do not always directly address juvenile fraud and hacking, the legal system has the tools (cyber law, communications regulation) to handle these problems.

The United States employs a dual approach in dealing with juvenile cybercrimes by merging basic cybercrime regulations like the Computer Fraud and Abuse Act at the federal

level alongside state-level juvenile justice systems emphasising rehabilitation. The federal law permits the prosecution of severe cybercrime offenses, but the state-level juvenile justice system places a greater emphasis on reform than incarceration, thereby striking a balance between the two, which ensures that young criminals bear responsibility for their actions while yet getting the support they need to rejoin society.

8. The Urgent Requirement for Change

Since the JJ Act was not designed with digital offences in mind, there is a need for targeted reform of the Act to incorporate cyber offences involving children that can be discussed in the following section:

8.1 Redefining Heinous Offences

The definition of "heinous offences" in the JJ Act should be expanded through an impact-based criterion. The current definition of "heinous offence" is based on the quantum of punishment (seven years or more). This approach does not adequately address cyber offences where the impact may be severe despite lower statutory penalties. Therefore, an impact-based evaluative framework must be adopted, taking into account the following factors-

- The extent of the harm done
- Characteristics of the crime
- Intention (Mens Rea)
- Repetition and scale
- Application of skills and technology
- The Victim's Vulnerability

8.2 Inclusion of Cyber-Specific Provisions

In the absence of cyber-specific provisions, the approach to cyber offences has been inconsistent with weak enforcement. So, adding cyber-specific provisions as procedural safeguards and capacity-building tools and not just punitive mechanisms becomes necessary in consonance with the rehabilitative philosophy of the JJ Act. With this in mind, some specific provisions are required to be incorporated in the Act, including-

- Procedures for managing electronic evidence
- Assessment of the child's technological capacity

Coordination with cybercrime units

8.3 Tailored Reformative/Rehabilitative Interventions

Reformative and rehabilitative measures under the JJ Act should address the unique nature of cyber offences for children involved in cybercrimes by balancing accountability with capacity building. Such measures must be individualised, proportionate, and development-oriented with the focus on reform through informed, content-specific interventions that should include the following:

- Technology use and ethics training
- Counselling for responsible internet use
- Skill redirection and constructive engagement (e.g., ethical hacking training)
- Parental accountability (Establishing a policy of parental responsibility in the rehabilitation process.)

8.4 Capacity Building

All parties involved in the juvenile justice system, including police officers, judicial officials, and members of Juvenile Justice Boards should be trained to handle cyber-related cases. The system needs continuous upskilling to keep pace with the technological advancement to strengthen the competencies of all stakeholders, which include the following:

- Providing specialized training of judicial officers and Juvenile Justice Boards
- Conducting awareness and sensitization programs for law enforcement personnel
- Create digital awareness among staff of child care institutions.

8.5 Inter-Agency Collaboration

A comprehensive strategy based on organized cooperation among many parties, is necessary when addressing cybercrimes relating to children which includes:

- Juvenile Justice Boards
- State Child Protection Units/District Child Protection Units
- Cybercrime cells
- Educational institutions
- Reformation homes/institutes

Besides, the Act should mandate standard operating procedures defining the roles and timelines of each agency, information sharing protocols, and accountability to achieve a coherent, child-centered system.

9. Conclusion

The increase of cyber delinquency presents a major challenge to the existing juvenile justice framework in India. While the emphasis on rehabilitation shows the progressive nature of the JJ Act, it fails to address this emerging form of cyber delinquency. Its reliance on a classification system based on punishment in conjunction with the absence of cyber-specific clauses in the Act accounts in part for this. This critical gap in the Act not only undermines the effectiveness of the justice system but also its rehabilitative objectives. Treating cyber offences as inherently less serious offence attracting lesser statutory penalties overlooks the potential to cause substantial harm, including psychological, financial, and societal impact, thereby limiting both responsibility and corrective measures.

In the face of rapid technological changes, the current framework cannot remain static, but the law must be reformed so that it will reflect the realities of the digital age. By adopting an impact-based classification approach, incorporating cyber-specific provisions, strengthening institutional capacity, and developing specialized rehabilitation programs, the juvenile justice system can more effectively balance accountability with reform. Ultimately, bridging this gap is essential to ensuring that the law remains responsive, relevant, and capable of addressing the complexities of modern criminal behaviour among children, while continuing to uphold its core objective of child-centric justice.

References

Abd Rahman Shah, H., Abdul Shukor, S., Mohamad Ali, N., Abdul Ghafar, A., Mohammad Ahmad, N., Yusof, N., & Atira Musa, N. (2018). Child delinquency on the Internet. International Journal of Engineering & Technology, 7(3.30), 320–324

Asiabar, M. G., Asiabar, M. G., & Asiabar, A. G. (2025). Legal and psychological analysis of juvenile criminal responsibility in cyberspace [Preprint]. Preprints.org. https://doi.org/10.20944/preprints202507.0484.v1

Binu Bihani. (n.d.). Characteristics of cybercrime. LinkedIn. https://www.linkedin.com/pulse/characteristics-cyber-crime-binu-bihani-7pknc

City of London Police. (n.d.). What is fraud? Report Fraud. https://www.reportfraud.police.uk/what-is-fraud/

Deb, A., & Chowdhury, P. R. (2018). A critical analysis of the Information Technology Act, 2000 vis-à-vis mitigation of child pornography. Christ University Law Journal, 7(2), 1–22. https://doi.org/10.12728/culj.13.1

Dwivedi, F., & Sharma, S. (2025). Strengthening legal frameworks for juvenile online safety: Evaluating cyber laws and policies. The Legalites Lexscripta, 1(2), 97–112

Gaur, S. K. (2025). Juvenile offender in the digital age: The role of social media. Indian Journal of Law and Legal Research, 7(4), 589-600

Goyat, R. (2025). Digital crimes and juvenile offenders: Legal gaps and policy challenges in India. International Journal of Information Movement, 9(X), 44-52

Information Technology Act, 2000 (India).

Jacob, P. (2025). Recidivism among juvenile offenders: Causes and prevention. International Journal of Creative Research Thoughts, 13(6), b869–b881.

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

Manoj, D., James, R. I., Kumaran, S., Devnath, G. P., Varughese, B. T., Arakkal, A. L., & Johnson, L. R. (2025). Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation. Child Protection and Practice, 4, 100088. https://doi.org/10.1016/j.chipro.2025.100088

Misra, P. K., & Tiwari, S. (2026). Cyber culture and juvenile justice: Rethinking legal frameworks for juvenile offenders in the cyber era. International Journal of Research in Social Sciences and Humanities, 16(1). https://doi.org/10.37648/ijrssh.v16i01.005

Paul, R. (2025, December 3). Juvenile justice in the age of cybercrime. Vintage Legal. https://www.vintagelegalvl.com/post/juvenile-justice-in-the-age-of-cybercrime

Press Information Bureau. (2026, April 1). Ministry of Women and Child Development is nodal Ministry for administration of Juvenile Justice Act, 2015. Government of India. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2247568

Saha, A. (2026, January 2). From IPC to BNS: What has really changed? Khurana & Khurana. https://www.khuranaandkhurana.com/from-ipc-to-bns-what-has-reallychanged

Sahajpreet Bhusari, (2021, September 14), Doli Incapax: Meaning, Origin, Explanation, Application and Important Case Laws, Legal Bites https://www.legalbites.in/doli-incapax-meaning

Santos, J. (2023, April 10). Promoting digital inclusion in juvenile detention facilities. IPS Innovative Prison Systems. https://prisonsystems.eu/promoting-digital-inclusionin-juvenile-detention-facilities

Viveka, S. (2024), Evaluating the Gaps in the Juvenile Justice Act, 2015 for Heinous Crimes: Adult Punishment v. Juvenile Justice, Indian Journal of Law and Legal Research,7(5), pp. 5344–5354