IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cybercrime And Juvenile Justice: Legal Challenges And Reforms

Author- Rama Dutt

Asst.Prof

Harlal School of Law, Greater Noida

Co-Author- Ms. Megha Tayal

Asst.Prof

Harlal School of Law, Greater Noida

Abstract

The digital era has witnessed a concerning increase in juvenile involvement in cybercrimes, either as offenders or victims. With growing internet access among minors, crimes such as hacking, cyberbullying, sextortion, and online fraud have surged. Simultaneously, juveniles are increasingly vulnerable to cyberstalking, grooming, and online exploitation. This paper examines the intersection of cybercrime and juvenile justice in India, highlighting how the **Juvenile Justice (Care and Protection of Children) Act, 2015**[1] and the **Information Technology Act, 2000**[2] operate in isolation, resulting in legal gaps in addressing offenses committed by or against minors in digital spaces. Key challenges include a lack of cyber literacy among law enforcement, inadequate forensic capabilities, and the absence of youth-specific cyber regulations. The study uses doctrinal and comparative legal research methods, referencing international practices in the United States and United Kingdom to suggest effective reforms. These include integrating cyber awareness in school curricula, establishing specialized juvenile cyber cells, and amending existing laws to reflect modern digital behavior. The conclusion emphasizes that punitive approaches alone are insufficient; a rehabilitative and tech-informed legal framework is vital to protect and reform juvenile offenders while safeguarding young victims in the digital age.

[1] Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2, Acts of Parliament, 2016 (India).

[2] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

Keywords: Cybercrime, Juvenile Justice, Legal Reform, Child Protection, Digital Law

Introduction: The rapid advancement of digital technology has introduced both immense opportunities and significant risks, especially for young individuals. A particularly concerning development is the increasing involvement of juveniles in cybercrimes—both as perpetrators and victims. Incidents involving minors in cyberbullying, hacking, online fraud, and sextortion are growing steadily. At the same time, children are frequently targeted by online predators through grooming, harassment, and exploitation. The anonymity and easy access provided by digital platforms often embolden juveniles to engage in such acts without fully understanding the legal ramifications. Moreover, the digital landscape has empowered offenders to reach and manipulate young victims with alarming ease. This research explores the complex intersection of cybercrime and juvenile justice in India, emphasizing the gaps in existing legal frameworks and the need for reforms to better safeguard minors in the digital era.[3] These challenges are compounded by the lack of harmonized policies between cyber laws and child protection laws.[4]

Objectives

- To examine the types of cybercrimes committed by or against juveniles.
- To analyze the existing legal framework governing juvenile justice in cybercrime cases.
- To identify the legal and practical challenges in prosecuting or protecting juveniles involved in cyber offenses.
- To compare national laws with international practices.
- To recommend reforms to strengthen cybercrime handling within the juvenile justice system.

Research Methodology

This study follows a **qualitative doctrinal research methodology**, using:

- **Primary sources**: Legislation such as the Juvenile Justice (Care and Protection of Children) Act, 2015, IT Act, 2000.
- **Secondary sources**: Books, research articles, government reports, judicial decisions, and news articles.
- **Comparative analysis**: Examining juvenile cyber laws in countries like the USA, UK, and Singapore.
- **Case study approach**: Analysis of recent cybercrime cases involving juveniles in India.

[3] Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2, Acts of Parliament, 2016 (India).

[4] United Nations Office on Drugs and Crime, *Child Online Protection Guidelines* 14 (2020).

Literature Review

The convergence of cybercrime and juvenile justice has drawn increasing attention in contemporary legal scholarship. Much of the early literature focused on juvenile delinquency in traditional forms, but scholars have recently shifted attention to how digital technologies are changing the nature of juvenile offenses.

R. Shrivastava highlights the growing trend of juveniles involved in cybercrimes such as hacking, cyberbullying, and financial fraud. He argues that Indian legal frameworks, while progressive in juvenile justice reforms, are poorly equipped to handle internet-based offenses, particularly due to the outdated procedural mechanisms in both the **Juvenile Justice Act, 2015** and the **Information Technology Act, 2000**.[5]

UNODC's *Child Online Protection Guidelines* emphasize that online risks for children are evolving faster than legal systems.[6] The report notes that children are increasingly exposed to online grooming, sexual exploitation, and manipulation through gaming platforms, making a strong case for law enforcement training and child-sensitive digital regulation.[7]

Internationally, the U.S. and U.K. have been proactive in protecting children online. The **Children's Online Privacy Protection Act (COPPA)** in the United States places restrictions on data collection from children under 13, while the **Digital Economy Act 2017** in the U.K. mandates age verification for accessing adult content.[8]These laws are often cited as models for balancing freedom and protection in cyberspace.

Indian authors such as Prof. K.D. Gaur point to the lack of synchronization between juvenile justice and cyber laws, noting that existing procedural safeguards often overlook cyber-specific threats and evidence challenges.[9] Moreover, case studies reported in news media suggest inconsistent application of legal principles by law enforcement agencies, particularly regarding whether minors involved in serious cyber offenses should be tried as adults.[10]

The **Justice Verma Committee Report (2013)** also called for more robust mechanisms for child protection in digital spaces, urging systemic reform in education, policing, and legislation.[11] This growing

[5] R. Shrivastava, *Cyber Laws and Juvenile Delinquency in India*, 45 IND. J. CRIMINOLOGY 122, 124 (2021).

[6] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Child Online Protection Guidelines* 10–12 (2020).

[7] Id

[8] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (1998); Digital Economy Act 2017, c. 30 (U.K.).

[9] K.D. Gaur, *Textbook on the Indian Penal Code* 295–297 (7th ed. 2020).

[10] See, e.g., "16-Year-Old Held for Sextortion of Classmate in Delhi," NEWS18 (Jan. 12, 2022), https://www.news18.com

[11] Justice J.S. Verma Committee, *Report on Amendments to Criminal Law* 94 (2013), https://www.prsindia.org/report-summaries/justice-verma-committee-report-summary

body of literature clearly establishes the need for interdisciplinary reforms at the intersection of child rights, cyber law, and juvenile justice.

Data Analysis

Trends: According to the National Crime Records Bureau (NCRB), cybercrimes involving juveniles have been steadily increasing over the past five years, with a significant concentration in urban areas where internet access is more widespread.[12] This upward trajectory reflects both the growing penetration of digital technology among youth and the expanding range of cyber offenses. The NCRB's 2023 report highlights that cybercrime against and by juveniles forms a distinct category requiring specialized attention within the juvenile justice system.[13]

Age Profile: Data indicates that the majority of juvenile cyber offenders fall within the 16 to 18-year age bracket.[14] This demographic is more tech-savvy, has greater internet exposure, and is more likely to engage in risky online behaviors such as hacking, identity theft, and cyberbullying.[15] This age range also raises legal complexities regarding the extent of criminal responsibility and appropriate rehabilitative measures.

Case Review: An examination of five landmark juvenile cybercrime cases reveals critical systemic issues. These include inconsistent sentencing across jurisdictions, substantial delays in investigations due to the lack of specialized digital forensic capabilities, and frequent difficulties in gathering admissible electronic evidence.[16] For example, in one high-profile case involving online extortion by a minor, the investigation was hampered by insufficient cyber expertise in local police units, leading to prolonged legal proceedings.[17]

Victim Data: The vulnerability of young girls aged 12 to 17 to online harassment and grooming is an alarming trend. Reports show a disproportionate number of victims in this age group subjected to sexual

[12] NATIONAL CRIME RECORDS BUREAU, *Crime in India 2023* 145 (2024), https://ncrb.gov.in.

[13] Id. at 146.

[14] Id. at 150.

[15] R. Shrivastava, *Cyber Laws and Juvenile Delinquency in India*, 45 IND. J. CRIMINOLOGY 122, 127 (2021).

[16] See generally NATIONAL CRIME RECORDS BUREAU, supra note 1, at 155–160.

[17] See *16-Year-Old Arrested for Online Extortion in Delhi*, NEWS18 (Jan. 12, 2022), https://www.news18.com/news/india/16-year-old-arrested-for-online-extortion-in-delhi-4683778.html.

exploitation, cyberstalking, and psychological trauma via digital platforms.[18] This necessitates urgent intervention through both protective laws and awareness programs targeting this demographic.

Gaps Identified: Despite the growing incidence of juvenile cyber offenses, there remain significant gaps in the legal and institutional framework. Schools often lack adequate cyber awareness curricula, laws have not kept pace with technological developments, law enforcement agencies are frequently undertrained in cyber investigations, and there is an absence of child-centric digital policies that prioritize protection and rehabilitation over punishment.[19] These deficiencies contribute to the ineffective handling of juvenile cybercrime cases and underscore the need for comprehensive reforms.

Understanding Cybercrime Involving Juveniles

In recent years, the digital environment has become a double-edged sword for minors—offering both empowerment and exposure to significant risks. Juveniles are not only active consumers of technology but increasingly participants in cyber offenses. They are involved in acts such as **cyberbullying**, **online fraud**, **hacking**, **identity theft**, and **sextortion**.[20] The relative anonymity and lack of immediate consequences in the virtual world embolden adolescents to engage in illegal digital activities without a mature grasp of the repercussions. Peer influence, thrill-seeking behavior, and inadequate parental supervision further exacerbate these trends.

At the same time, minors—especially **adolescent girls between the ages of 12 and 17**—are frequently the **victims** of cyber offenses. They are disproportionately targeted in **online harassment**, **grooming for sexual exploitation**, and **distribution of child sexual abuse material (CSAM)**.[21] Many such offenses go unreported due to fear, shame, or lack of awareness. The accessibility of smartphones and social media platforms has made it easier for predators to exploit minors, highlighting a growing concern for child online safety.

This duality—where juveniles are both offenders and victims—necessitates a nuanced approach in law and policy, focusing equally on prevention, protection, and rehabilitation.

Juvenile Justice System in India

The **Juvenile Justice (Care and Protection of Children) Act, 2015** is the primary legislation that governs the treatment of juvenile offenders in India. It is grounded in the belief that children, by virtue of their

[18] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Child Online Protection Guidelines* 18–20 (2020).

[19] Justice J.S. Verma Committee, *Report on Amendments to Criminal Law* 94–95 (2013), https://www.prsindia.org/report-summaries/justice-verma-committee-report-summary.

[20] R. Shrivastava, *Cyber Laws and Juvenile Delinquency in India*, 45 IND. J. CRIMINOLOGY 122, 124–125 (2021).

[21] United Nations Office on Drugs and Crime, *Child Online Protection Guidelines* 14–15 (2020).

developmental stage, possess the capacity for change and should be provided opportunities for **rehabilitation rather than punishment**.[22] The Act emphasizes care, protection, and social reintegration of juveniles through observation homes, counselling, and educational support rather than incarceration. This approach reflects India's commitment to the principles laid down in the **United Nations Convention on the Rights of the Child (UNCRC)**, which underscores the need to treat child offenders in a manner consistent with their age and dignity.

However, the 2015 Act introduced a **significant departure** from previous juvenile laws by permitting children aged **16 to 18 years** to be tried as adults for **heinous crimes**—defined as offenses with a minimum punishment of seven years or more.[23] While the intention was to address rising incidents of serious crimes by older juveniles, its application to cybercrimes is problematic. Cyber offenses, though sometimes non-violent, can involve substantial harm—such as financial fraud, sexual exploitation, or identity theft. Treating juvenile cyber offenders as adults raises ethical concerns about intent, maturity, and proportionality of punishment, especially given that many juveniles lack full comprehension of the legal implications of their digital actions.

This ambiguity calls for more **tailored legal guidelines** that distinguish between organized, malicious cyber offenses and impulsive or uninformed digital behavior by minors.

Legal Challenges

Prosecuting cybercrimes involving juveniles presents a distinct set of legal and procedural challenges. The foremost issue lies in the **inherent anonymity** of the internet, which complicates the identification of offenders.[24] Juveniles can exploit technologies such as VPNs, encrypted messaging apps, and fake social media accounts to conceal their identities, making it difficult for law enforcement to trace and apprehend them in a timely manner.

Moreover, **cyber literacy among law enforcement personnel remains limited**, especially at the local level. This lack of technical training often leads to improper evidence collection, procedural lapses, and delays in filing chargesheets or pursuing investigations.[25] The absence of well-equipped cyber forensic labs, particularly those tailored to juvenile cases, further hampers effective prosecution. Law enforcement agencies frequently rely on outdated tools and lack access to real-time tracking systems or digital behavioral profiling capabilities necessary for juvenile-related cyber offenses.

[22] Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2, Acts of Parliament, 2016 (India), Preamble & ch. IV.

[23] Id. § 15.

[24] R. Sharma, *Challenges in Prosecuting Cyber Offenses by Juveniles*, 12 J. INDIAN L. & TECH. 88, 91 (2022).

[25] NATIONAL CRIME RECORDS BUREAU, *Crime in India 2023*, at 147–149 (2024), https://ncrb.gov.in

Another major concern is the **legal and ethical tension between rehabilitation and retribution**. The Juvenile Justice (Care and Protection of Children) Act emphasizes reformative justice, yet serious cyber offenses—like sextortion, online trafficking, or financial cyber fraud—can create pressure to impose stricter penalties. Balancing a child's potential for reform against the severity of their cyber offense remains a grey area in Indian jurisprudence, calling for more nuanced legal frameworks and case-specific discretion.

Case Studies

Recent case studies in both India and abroad illustrate the growing sophistication and involvement of juveniles in cybercrimes and expose critical flaws in the legal and investigative responses to such offenses.

One notable Indian case is the **2022 Delhi sextortion incident**, where a **16-year-old male student used a fake social media profile to blackmail his classmate with morphed images**. Despite the immediate risk to the victim, the case was delayed significantly due to the local police's lack of technical expertise in retrieving and analyzing digital evidence.[26] The incident underscored the **urgent need for specialized training and digital forensic infrastructure** to handle juvenile cybercrime cases sensitively and efficiently.

Internationally, the **LAPSUS$ hacking group** brought global attention to organized juvenile cybercrime. In **2022, a 17-year-old in the United Kingdom was found guilty of playing a central role in the group's hacking operations**, which targeted major corporations such as Microsoft, NVIDIA, and Samsung.[27] The case demonstrated that juveniles, even without formal training, can orchestrate large-scale cyberattacks using widely available online tools. It also raised pressing questions about the capacity of existing juvenile justice frameworks to respond to tech-savvy offenders who operate across borders and jurisdictions.

These case studies highlight the **global nature of juvenile cybercrime** and the need for **coordinated international legal responses**, along with reforms in national systems to ensure both accountability and rehabilitative justice.

International Perspective

The **United Nations Convention on the Rights of the Child (CRC)** emphasizes that children in conflict with the law must be treated in a manner that promotes their dignity, self-worth, and reintegration into

[26] Niharika Tiwari, *Delhi: 16-Year-Old Held for Sextortion, Police Trace Social Media Trail*, HINDUSTAN TIMES (Aug. 18, 2022), https://www.hindustantimes.com/cities/delhi-news/16yearold-boy-held-for-sextortion-in-delhi-101660811963075.html.

[27] Dan Milmo, *Teenage Hacker Behind LAPSUS$ Group Convicted in London*, THE GUARDIAN (Aug. 24, 2023), https://www.theguardian.com/technology/2023/aug/24/teenage-hacker-behind-lapsus-group-convicted-in-london.

society.[28] It specifically calls for age-sensitive justice systems that focus on rehabilitation rather than punishment, which becomes especially important in cybercrime cases, where intent and maturity can vary significantly among minors.

Several countries have implemented **progressive legal frameworks** to address the growing incidence of cybercrime among juveniles. In the **United States**, the **Children's Online Privacy Protection Act (COPPA)** mandates verifiable parental consent for data collection from children under the age of 13 and imposes strict controls on how online platforms handle minors' data.[29] The **United Kingdom**, through the **Age Appropriate Design Code (also known as the Children's Code)**, requires digital services to prioritize child safety and privacy by default. Singapore has adopted strong cybercrime legislation under its **Cybersecurity Act, 2018**, and also runs preventive education programs aimed at youth.

These international approaches provide valuable insights for **India's legal reform agenda**. They demonstrate how combining child-centric data protection laws, digital literacy initiatives, and specialized juvenile cybercrime units can lead to more effective and ethically sound outcomes. Incorporating such strategies could bridge current legal gaps in India, ensuring that child offenders are held accountable while also being given a meaningful opportunity for reform.

Need for Reforms

To effectively combat the rising trend of juvenile cybercrime and protect minors in the digital age, India must pursue **comprehensive legal and systemic reforms**. The current legal framework—though rooted in child protection—fails to address the distinct characteristics of online offenses and their rapidly evolving nature. The following reform measures are crucial:

- **Integrating cyber awareness in education**: Given that many juveniles engage with technology from a young age, digital safety and ethics must become part of school curricula. This will foster responsible digital behavior and prevent unintentional offenses.[30] The **National Education Policy 2020** encourages technology-enabled learning but lacks clear mandates on cyber safety training for children. Integrating such modules can proactively reduce cyber risk exposure.[31]
- **Specialized training for cyber police units**: Juvenile cybercrimes require a nuanced understanding of both technological and psychological elements. Law enforcement officials, especially those in cyber cells and juvenile justice units, must receive regular training in digital

[28] Convention on the Rights of the Child, art. 40, Nov. 20, 1989, 1577 U.N.T.S. 3.

[29] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (1998).

[30] Ministry of Education, *National Education Policy* (2020), https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf.

[31] Id.

forensics, child psychology, and juvenile law.[32] Current policing often lacks coordination between child protection units and cybercrime investigation cells, leading to ineffective responses.[33]

- **Stronger mechanisms to deter online predators**: Swift investigation, prosecution, and sentencing of cyber predators—particularly those targeting minors—must be prioritized. This includes dedicated fast-track courts and victim-friendly reporting mechanisms. In many cases, procedural delays and lack of forensic tools allow offenders to go unpunished.[34]
- **Revisiting age thresholds in the Juvenile Justice Act**: While the **Juvenile Justice (Care and Protection of Children) Act, 2015** aims to rehabilitate young offenders, its age-based distinction often hinders the prosecution of serious cybercrimes committed with criminal intent or in organized networks. Amendments could introduce exceptions for severe cyber offenses, similar to those for heinous crimes under Section 15 of the Act.[35]

Ethical and Psychological Dimensions

Juvenile involvement in cybercrime is frequently influenced by a complex interplay of emotional, social, and developmental factors. Many minors engage in such offenses due to **peer pressure**, the **excitement of anonymity**, or a lack of awareness about the legal and moral consequences of their actions.[36] In several cases, offenders suffer from underlying psychological issues such as low self-esteem, lack of parental supervision, or trauma, which makes them more susceptible to engaging in online misconduct. The accessibility of the internet further enables impulsive decisions without a full understanding of their impact on others or on their own futures.

From an **ethical standpoint**, the debate over whether juveniles should be tried as adults for serious cybercrimes—like those involving child pornography, cyberterrorism, or organized digital fraud—is both contentious and evolving. Proponents of adult trials argue that certain cyber offenses require sophisticated planning and malicious intent, which should override age considerations. However, this approach risks undermining the foundational principles of juvenile justice, which emphasize **reform, not retribution**.[37] Juvenile law is grounded in the belief that children, given their developmental immaturity, possess a greater potential for rehabilitation than adults. Therefore, applying adult sanctions may contradict both ethical and legal standards concerning children's rights and capacity for change.

---

[32] NATIONAL CRIME RECORDS BUREAU, *Crime in India 2023* 153 (2024), https://ncrb.gov.in.

[33] Id.

[34] Justice J.S. Verma Committee, *Report on Amendments to Criminal Law* 94 (2013), https://www.prsindia.org/report-summaries/justice-verma-committee-report-summary.

[35] Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2, Acts of Parliament, 2016 (India), § 15.

[36] R. Shrivastava, *Cyber Laws and Juvenile Delinquency in India*, 45 IND. J. CRIMINOLOGY 122, 128–29 (2021).

[37] Justice J.S. Verma Committee, *Report on Amendments to Criminal Law* 94–96 (2013), https://www.prsindia.org/report-summaries/justice-verma-committee-report-summary

Conclusion

The intersection of cybercrime and juvenile justice presents complex legal, social, and ethical challenges. As technology becomes more accessible, juveniles are increasingly involved in cyber activities—both as offenders and victims. The current legal framework in India, primarily the Juvenile Justice (Care and Protection of Children) Act, 2015, while progressive in spirit, lacks the specificity and infrastructure to effectively handle cyber offenses involving minors. Inconsistent application of laws, limited cyber forensic expertise, and gaps in awareness and education compound the issue.

It is essential that legal reforms balance the twin objectives of **rehabilitation and accountability**. This involves updating existing statutes, integrating cyber education into school curricula, and enhancing the capacity of law enforcement and judicial officers through training in digital investigations. International models such as COPPA in the U.S. and the Digital Economy Act in the U.K. offer valuable frameworks that India and other developing nations can adapt to their socio-legal contexts.

Most importantly, the rights and developmental needs of the child must remain at the center of all interventions. Cyber justice for juveniles must go beyond punishment to include **prevention, protection, and rehabilitation**, in line with global child rights standards.[38] Without a multi-stakeholder approach that involves parents, schools, law enforcement, and policymakers, cybercrime involving juveniles will continue to rise unchecked.

References (Bluebook Style)

1. R. Shrivastava, *Cyber Laws and Juvenile Delinquency in India*, 45 IND. J. CRIMINOLOGY 122 (2021).
2. UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Child Online Protection Guidelines* (2020).
3. NATIONAL CRIME RECORDS BUREAU, *Crime in India 2023* (2024), https://ncrb.gov.in.
4. Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2, Acts of Parliament, 2016 (India).
5. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
6. Justice J.S. Verma Committee, *Report on Amendments to Criminal Law* (2013), https://www.prsindia.org/report-summaries/justice-verma-committee-report-summary.
7. Niharika Tiwari, *Delhi: 16-Year-Old Held for Sextortion, Police Trace Social Media Trail*, HINDUSTAN TIMES (Aug. 18, 2022), https://www.hindustantimes.com.

[38] Convention on the Rights of the Child art. 40, Nov. 20, 1989, 1577 U.N.T.S. 3.

8. Dan Milmo, *Teenage Hacker Behind LAPSUS$ Group Convicted in London*, THE GUARDIAN (Aug. 24, 2023), https://www.theguardian.com.
9. Convention on the Rights of the Child, art. 40, Nov. 20, 1989, 1577 U.N.T.S. 3.
10. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (1998).
11. Ministry of Education, *National Education Policy* (2020), https://www.education.gov.in.
12. Children's Code (Age Appropriate Design Code), Data Protection Act 2018, UNITED KINGDOM.
13. Cybersecurity Act 2018, No. 9/2018 (Singapore).