



Exploring Legislation, Constitutionality, Cybercrime, and Sciences: A Cinematic Analysis and Interpretation of Juvenile Justice, in the Digital Age

Prasanna Nandanwar

Student, Symbiosis International University

Corresponding Author Email ID: prasanna.nandanwar2924@gmail.com

Abstract

This analytical paper undertakes an extensive, critical, and comprehensive examination of the juvenile justice system, with a particular focus on the legal disparities, legislative framework, interpretation, and its socio-legal ramifications. This study will scrutinize the child-centric statutes, ancillary legislations, and cybercrime jurisprudence to analyse their alignment in both conceptual and operational manner. The paper explores the legislation through fictional cinematic narration and real-life examples to evaluate whether it contextualizes itself to the societal and jurisprudential reality as it majorly focuses on section 15 of the Juvenile Justice (Care and Protection of Children) Act, 2015 which empowers the juvenile justice board to determine whether children aged 16-18 should be tried as adults for heinous crime constituting cyber offences. It tries to investigate the coherence of Indian legislative developments and implementation efficacy, and every possible hurdle in between, as it looks into the amendment brought about because of the public outburst in the *Nirbhaya case*, and its implications. The analysis is further drawn in conjunction with legislative reforms and the international convention to establish the intention of the lawmakers, nationwide institutionalization, and safeguards. The author, going forward, brings foreign juvenile systems, frameworks, and reforms in an attempt to study how other countries deal with juvenile delinquency. The conclusive aim of the research is to bridge the subject to its principal values of rehabilitation and reintegration with solutions, emphasizing fundamentally the constitutional mandate to uphold the child's best interests as it focuses on section 15 of the Juvenile Justice (Care and Protection of Children) Act, 2015.

Keywords: Juvenile Justice Act, UNCRC, Cybercrime, Juvenile Delinquency, Heinous, Constitutional Rights, and Reforms

Category:
Research Paper

Paper Code:
CUKJLS2502

Accepted on:
September 12, 2025

Introduction

"When society turns a blind eye to the roots of juvenile delinquency, it unknowingly shapes its own predators." India unlike other developing countries had been actively framing welfare laws in 20th century as well as adapting them to the societal and academic standards till 21st century, such as (for this paper), the Juvenile Justice Act of 1986 to the law in force, Juvenile Justice (Care and Protection of Children) Act of 2015 (herein after referred as JJ Act, 2015), but when the law fails to keep up with technology, justice becomes a game of control. The Information Technology Act, 2000 (herein after referred to as IT Act, 2000) (Information Technology Act, 2000 with its respective amendments, such as IT (Amendment) Act, 2008 still lacks far behind in the nuances of technology it promises to protect its people from. The International Convention taken into consideration involving children is the United Nations Convention on the Rights of the Child (UNCRC), as it articulates civil, political,

economic, social, and cultural rights of children. However, it remains deficient in conjoining the expansive digital threats a child may cause or suffer. Moreover, the 2 imperative national laws operate in isolation from one another, lacking cohesion; the objectives of these laws divergently differ when viewed through the lens of our justice system. The JJ Act, 2015, is primarily welfare-oriented; it aims to protect, rehabilitate, reintegrate, and reform the "*child*", whereas the IT Act, 2000, is predominantly punitive and regulatory in nature; it penalizes the "*accused*" it aims to protect the digital system. This shows how legislation, even in its true legal spirit when harmoniously constructed, becomes ill-equipped to deal with the Pandora's box.

It is fundamental to understand that technological advances permeate and grow in all spheres of human activities; individuals, more specifically, children, get themselves positioned as potential perpetrators and victims in this very cyberspace. This study will examine how existing legislation



ought to be interpreted in the light of socio-legal obstacles faced by India, while ensuring adherence to constitutional principles and preserving the integrity and objectives of child welfare.

The History of the Juvenile Justice System

The Act exhaustively, from the beginning, defines under Section 2(12) “child” means a person who has not completed eighteen years of age (Juvenile Justice Act, 2015). The 1986 Act had categorized its subject, the child, into 2 different categories based on the legislative intent. The core objective of the act was to safeguard the children, addressing their unique nurturing needs. The children who had suffered abandonment, torture, neglect or direly needed protection and safety due to abuse were called Children in Need of Care and Protection and others who were committing offences as defined in (now) Bharatiya Nyaya Sanhita, 2023 to be punished in a reformatory manner, such children were called Children in Conflict with the Law, these categorization enabled the children to appropriately be supported as well as reintegrated into society as they grow (Adusumilli, 2024). This categorization is still followed, as the Act applies to children aged 18 years and below. Indian legislators in 2000 introduced the Juvenile Justice (Care and Protection of Children) Act, becoming a ratified signatory to the *United Nations Convention on the Rights of the Child (UNCRC)*. This created a parallel of international standards to national law. It became the sole skeletal umbrella legislation that prioritized family-based care and reformation of the children under its jurisdiction, while barring the death penalty and imprisonment of any kind for juveniles. This act was able to deinstitutionalize formal adjudication and instead provided a fluid institution that focused on treating the needs of children, plus fostering a child-friendly approach. The act is inspired primarily by American jurisprudence of the juvenile justice system by following the doctrine of *parens patriae*, which signifies that the protection and rehabilitation is the guardian's responsibility that falls on the state ultimately (Mack, 1909). However, the paper tries to examine the shift of this welfare approach to a ‘rights and duties’ based approach, relying on its emphasis on constitutional rights at the forefront.

The society develops in both light and darkness; the 2012 *Nirbhaya gang-rape case* shocked the nation and haunted its people for decades to come, resulting in public outrage, riots, and protests. The case of *Mukesh & Anr v. State for NCT of Delhi*

(commonly referred to as the *Nirbhaya gang rape case*) represents a pivotal moment in Indian legal history, particularly in juvenile justice reform. This case exemplifies the tension between public sentiment, the principles of juvenile justice, and the State's constitutional and international obligations (Adusumilli, n.d., p. 7). What resulted for the Indian legal system and the 6 accused, including a minor, was public demand for the death penalty, the Criminal Law (Amendment) Ordinance, 2013, and the Juvenile Justice (Care and Protection of Children) Bill, 2015. Subsequently, the Parliament passed the bill, aiming to address public concerns and socio-criminal accountability for juveniles committing heinous offences. Upon enactment, the bill was called the Juvenile Justice (Care and Protection of Children) Act of 2015, which remains in force to date.

The most significant change was empowering the Juvenile Justice Board, under section 15, to determine adolescents/juveniles between the ages of 16 to 18 who had been accused of heinous crimes to mandatorily have a preliminary assessment. This assessment is determinant in deciding whether the child will be tried as an adult or not. The new act seemed to have resolved the issue raised by the public outrage over the appropriateness of the age limit of 18, for levying to criminal liability, especially in heinous offences.

In generic terms, juvenile delinquency has been defined as deviant child behaviour. When a young person is involved in a criminal act, he is referred to as a juvenile delinquent, juvenile offender, or youthful offender, and the crime, as juvenile delinquency (Nieborg et al., 2000, p.20). This terminology will be applied irrespective of the nature of the offence, including heinous, petty, serious, economic, cyber, or narcotic crimes.

The Elemental Concept of Cybercrime

In basic understanding, Cybercrime, a.k.a computer-oriented crime, is construed as criminal activity that involves a computer and a network either as an instrument, target, or a means for perpetuating illegal acts, where unlawful acts are conducted only through a computer or similar, and is either a tool/medium or a target or both. Cybercrime has a broad nature of applicability as it can potentially threaten an individual, a company, private entities, a financial institution, or state security, all the while surpassing national borders. Cybercrime involves unlawful acts such as the commission of fraud, identity theft, privacy

violations, financial fraud, or intellectual property trafficking.

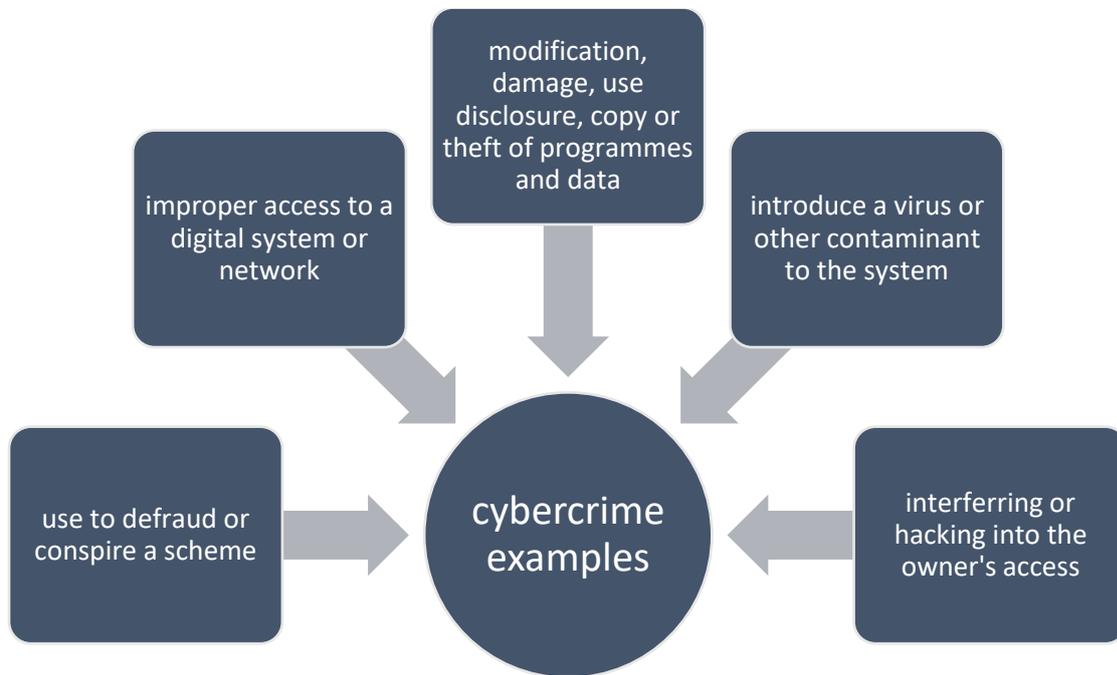


Fig. 2.1: What Constitutes a Cybercrime (Self-Created)

Cyber law exists in the municipal sphere to punish unauthorized access done with criminal intention and also prevents any future commission of the same. These crimes rely on the data network and the internet, and therefore, they leave zero physical evidence and little digital evidence. Cybercrimes do not require physical force by the accused; all it needs is a high-speed network for a few minutes for commission, which today is in boon and no more a luxury. This creates an enormous burden on law enforcement authorities, and it also consumes a long time because of the inability to locate them. It becomes difficult to decide and locate the jurisdiction for investigation powers and conviction procedures. These crimes can only be conducted by skilled individuals, and

these skills have no parallel of severity with age. The paper is focused on this peculiar characteristic of cybercrimes to place liability and facilitate rehabilitation in the spirit of the JJ Act, 2015. The IT Act, 2000 made provisions to prevent computer and network-based crimes, as well as giving protection of privacy, following the IT (Amendment) Act, 2008 where the parliament inculcated concepts like cyber terrorism (Section 66F), identity theft (Section 66C), and data protection (Section 72A), creating a liability/accountability-based legislation (ICLG, 2024). The different types of cybercrimes punishable under the BNSS, 2023, and IT Act, 2000 that are relevant to the study where Children can be Offenders in Cybercrime are:

Table 2.1: Types of cybercrimes and their punishments as per Indian law, IT Act, 2000

Section /laws	Punitive charge	Punishment
43	Penalty for damage to the computer, computer system, or network	Imprisonment up to 3 years and/or fine up to ₹2 lakhs
66	Computer-related offenses	Imprisonment up to 3 years and/or fine up to ₹5 lakhs
66C	Identity theft	Imprisonment up to 3 years and/or fine up to ₹1 lakh
66D	Cheating by personation using computer resources	Imprisonment up to 3 years and/or fine up to ₹1 lakh



66E	Violation of privacy	Imprisonment up to 3 years and/or fine up to ₹2 lakh
66F	Cyber Terrorism	Life imprisonment
67 and 67B	Publishing or transmitting obscene material in electronic form	Up to 5 and 7-years imprisonment and/or fine up to ₹10 lakh
69	Power to intercept, monitor or decrypt information	Imprisonment up to 7 years and fine
72A	Punishment for disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to ₹5 lakh
BNS, 2023	Certain cyber offenses are also covered under traditional criminal law (e.g., defamation, cheating). Cheating by personation using technology (under BNS Sections 316–318) Cyberstalking (under BNS Sections 78)	May extend Up to 7 years imprisonment;

Anand (2023) discusses the evolving landscape of cyber laws in India and explores the lacuna and its implications of an incomplete comprehensive legislation that can define every type of cybercrime, and therefore it is branchingly interpreted, to meet the needs of a wrongful act or offence. India in 21st century needs to go above and beyond existing laws and assert better cyber forensics to justly adjudicate these crimes national cyber security policy, 2023 is no capable legislative tool, erstwhile the rates of cybercrime will keep on increasing, making digital space unsafe for all kinds of vulnerable sections of society, specifically the children mentioned in JJ Act, 2015, as they can be both perpetrators and victims.

As previously discussed, cybercrimes have jurisdictional issues as well due to a lack of physical evidence and establishing *lex causae*. When the accused of a cybercrime is identified as a child in conflict with law, the jurisdiction is automatically conferred to JJB, Juvenile Justice Board (JJ Act, 2015). This applies irrespective of the nature of the offence. The composition of JJB under section 4 (JJ Act, 2015) is of JMFC, Judicial Magistrate of First Class, and social workers. However, it's concerning how both lack institutional capacity to adjudicate complex, high-value cyber offences, the requisite wisdom to comprehend cybercrimes or their psychological elements. Neither the presiding officer nor the social worker are typically equipped with the specialised technical and forensic understanding necessary to fully grasp the sophisticated nature of modern cybercrimes. Consequently, assuming that if the juvenile is accused is involved in causing substantial economic loss, amounting to millions of rupees, it may fundamentally fall beyond the functional and technical competence

of the JJB and preliminary assessment test conductors. The analytical question of commission of cyber and economic offences without understanding the consequences of a constitutionally disputed law is a threat to principles of justice, equity, and good conscience. The board should be perceived as being inability to respond to Juvenile delinquency; it is ill-equipped to determine and adjudicate this new breed of delinquency.

The Juvenile Justice Conundrum and Constitutional Validity.

The JJ Act, 2015 came into force by deriving legitimacy from Article 14 and 15(3) of the Constitution of India (Constitution of India, 1950, art. 21), which empowered parliament to enact this special legislation made for the welfare of the “child”. Acknowledging their unique developmental needs and the enhanced safeguards that this vulnerable segment of the population requires. On the other hand, this legislation now provides for the transfer and prosecution of heinous crimes committed by children aged 16 to 18 years to the children’s court when found to conflict with the law after a mandated preliminary assessment conducted by court-appointed professionals to be tried as an adult with formal procedures. This provision deviates from the inception *principle of child welfare*. When referring to Singh (2019) critically examining Section 15 of the Juvenile Justice Act, 2015. The JJ Act, 2015, further in section 3, postulates fundamental principles that should be followed whenever the act has any operation. The legislators and the judiciary, through various case laws and as Venkatesan (2021) reported, have clarified that the state bears a duty and obligation to uphold justice, public order, and have an



effective response to criminal offences committed within the state, even when the alleged perpetrators were juveniles, the very law aims to protect. The clarification was based on how these punitive provisions were to aid reformation and rehabilitation in the long run. The Act and its principles bring us to a crossroads, the principle of best

Bound by the laws of that time, the Juvenile Justice board had no other option than to give the maximum sentence: three years in a reformatory home to the accused minor of the *Nirbhaya case*. On appeal to the Supreme Court, the hon'ble Court upheld the JJ Act, and the punishment the Board had given. The rationale the court provided was that the Act envisaged its legislative intent and India's obligations under international law, particularly the United Nations Convention on the Rights of the Child (UNCRC). The Court reiterated that juveniles, due to their developmental immaturity and greater capacity for reform, must be treated differently from adults under the justice system (*Dr. Subramanian Swamy v. Raju*, 2014). The Supreme Court's rationale underscored the rule of law, emphasizing that legal principles and legislative frameworks must prevail over public sentiment to ensure fairness and consistency (*Mukesh v. State for NCT of Delhi*, 2017). *"In the age of technology, where every click and every keystroke leaves a mark, justice is no longer confined to the physical world; it bleeds into the digital, leaving us questioning what accountability truly means."* Using the definition of child and allowing the discrimination on subjective analysis violates Article 14, 15(3), and 21 of the Indian Constitution. As held in *E.P. Royappa v. State of Tamil Nadu* (1974) that arbitrariness is the sworn enemy of equality. With that precedent, the arbitrariness in the JJ Act is unconstitutional as it violates the Fundamental Right of equality before law and equal protection of law. The Act classifies offences as **petty, serious, and heinous**, but many BNS offences do not clearly fall in these categories. This creates legal confusion, and conviction on legal confusion is against the principles of criminal law, such as *Nullum crimen, nulla poena sine lege*, and *Presumption of Innocence*, which ensure that no innocent individual can be punished for an act unless it is defined and can be strictly or literally interpreted as a crime by law.

Mental Age and Psychology

Despite being popularly viewed as revealing the "objective truth," neuroimaging techniques involve an element of subjectivity (Johnson,

Blum, and Giedd,2009). The JJ Act, while mandatorily conducting a preliminary assessment for children aged 16 to 18 years when accused of heinous Crimes, is a subjective assessment. It burdens psychologists and other members with an erroneous obligation to measure a child's mental capacity. Which to *Pickles, Edwards, Horvath, and Emsley's (2023)* research of novel methodology, neurodevelopment, and medical sciences, with an evidence-based study determine that even with modern technology is become impossible to conclusively determine the mental capacity of a child. While *Johnson, Blum, and Giedd (2009)* discuss and provide the implications of adolescent brain development from the purview of neuroscience. Their research shows that even when there are policies, theories and developed technology in the neuro-imaging and current neurosciences, one cannot reliably determine the behavioural and decision maturity at the individual age level.

"Age-based policies are not exceptional; policies are frequently enacted in the face of contradictory or non-existent empirical support. Although neuroscience has been called upon to determine adulthood, there is little empirical evidence to support age 18, the current legal age of majority, as an accurate marker of adult capacities. Less clear is whether neuroimaging, at present, helps to inform age-based determinations of maturity." (*Johnson, et al,2009*)

These academic findings underscore and lapse the preliminary assessment under section 15 of the JJ Act,2015, and establish that brain development is a continuous variable and context-dependent process, significantly influenced by socio-economic and environmental factors. In conclusion, neuroscience and psychology do not support a rigid age-based cutoff for determining maturity, given the substantial inter-individual variation in cognitive and psychosocial development.

Additionally, Objective evaluations based solely on preliminary or age-based assessments are **scientifically unreliable**, as they fail to capture individual variability, situational influences, or developmental complexity.

The entirety of the universe and its scholars have only been able to label and recognize the symptoms of various underlying, overlapping, and prima facie mental health issues or disorders, allowing assessment of such a fractured pool of understanding hampers the constitutional rights of the "child".



International Covenants on Juvenile Justice and Cybercrime

In no clearer words of law ever, the UN Convention on the Rights of the Child (UNCRC), 1989, in its Article 1, defines a *child* as anyone under 18 years of age undisputedly. UNCRC, 1989, lays the foundation for treatment for children in conflict with the law it enforces, under Article 40, that the juvenile justice system must recognize the rights of children brought before it on the allegation of violating penal laws and maintain their dignity in consonance with their age. This international law can be widely interpreted to be “**Balancing Accountability and Child Rights**” to even be followed for cyber juveniles who are found to conflict with the law. Under this law, when children are cyber offenders, states are required to:

1. Ensure fair legal processes (Article 40, UNCRC).
2. Consider psychological and social maturity before applying criminal liability.
3. Emphasize reform over retribution.
4. Provide access to legal counsel and protection from undue detention.
5. Address root causes like lack of digital literacy or online grooming.

“Rule 2.2 defines “Juvenile” and “offence” as the components of the notion of the “juvenile offender”, who is the main subject of these Standard Minimum Rules (see, however, also rules 3 and 4). It should be noted that age limits will depend on, and are explicitly made dependent on, each respective legal system, thus fully respecting the economic, social, political, cultural, and legal systems of Member States. This makes for a wide variety of ages coming under the definition of “juvenile”, ranging from 7 years to 18 years or above. Such a variety seems inevitable in view of the different national legal systems and does not diminish the impact of these Standard Minimum Rules.” (Beijing Rules, 1985, Rule 2.2)

The Beijing rules, therefore, refer and draw similarity that offenses committed by adults would also reflect offenses committed by juveniles but shall only be handled by specially empowered juvenile justice systems, making differential treatment a valid legal discrimination. The enunciates and delineates how international law’s concept of delinquency hinges not just on age (typically under 18), but also on the legal treatment framework applied to the offender. These rules also focused on education and restorative justice instead of punishment.

The Indian jurisprudence also follows in spirit the United Nations Guidelines for the Prevention of Juvenile Delinquency (Riyadh Guidelines), 1990, which is majorly focused on **preventive measures** to reduce juvenile delinquency. *It states that “behaviour by children and young persons which may result in contact with the juvenile justice system.”* To be a delinquent behaviour, under the spectrum of cybercrimes, the juvenile justice system can adopt and encourage the juveniles committing cybercrimes to have *Positive socialization* with the help of a child welfare officer. Khan and Gulati (2023) compare the cybercrime legislation frameworks of India, Israel, and the USA and show how India lacks the appropriate legislation to tackle cybercrime threats made by juveniles.

Case studies based on cinematic narration and real-life examples

The case studies are imperative to be analyzed as cybercrime in India has its challenges as referred to and explained by Iqbal and Beigh (2017), and presents the technological responses. In early 2025, The Times of India (2025) reports that the Kochi city cyber police were able to arrest 2 men of Varanasi who partook in a nationwide online fraud of operating a fake government parivahan application, which made residents of Ernakulam alone pay vehicle fines under misinformation of about 85,000 rupees. Upon investigation, a juvenile of 16-year-old was traced to be the mastermind who also made the fake applications and challans via telegram to defraud the people. However, no arrest or preventive detention could be made against this child as the JJ Act, 2015 had exclusive jurisdiction, which has its own child welfare police officers that could take cognizance of this matter. Now these cases question whether the juvenile justice framework adequately balances the need for societal justice and deterrence with the potential for rehabilitation and reform of juveniles. Conjunctionally questioning whether the Hon’ble Welfare Adjudicating Institution is equipped and capable of carrying and sorting this tangled bundle of threats and precautionary steps.

Further **USA swatting case**, where a 16-year-old had caused national security panic while making fake calls, also known as the **Alan Winston Filan case**. The Facts are as follows: the case lasted from August 2022 to January 2024. The accused Filan, is from Lancaster, California. On May 12th, 2023, police in Florida got a chilling 911 call.

The caller sounded shaken up, claiming life-threatening situation in the background. The 911



operator heard loud popping noises that sounded like fireworks or something worse. Before hanging up, the caller gave one crucial piece of information: his location. Within minutes, 30 armed officers were on their way. They expected chaos, maybe even a violent Showdown, but when they arrived, everything was calm. No one was in danger, and no one was hurt. The cops, after talking to a few people in the neighbourhood they realized what had happened: the 911 call was a prank, a fake emergency. The officers went back to the station, hoping this would be a one-time thing, but it wasn't. The same person called 911 again and again, each time with a different voice, a different number, and a different story, but every time police rushed to the scene, they realized no one was in danger. In some cases, the 911 caller sent police to people's homes, the cops would break through the doors scaring those who lived there, little did they know the call they were hunting was just a teenager. Alan Winston Filan made his first swatting call in August 2022. He used text-to-speech software to disguise his voice and caller ID spoofing to hide his location. When police fell for it the first time, Filan felt a rush of excitement.

He realized he could outsmart the system. Soon Allen started swatting bigger targets schools, churches, and military bases. He even sent SWAT teams to the homes of FBI agents and US senators. He's allegedly targeted Washington State, Texas,

Florida, and Maryland. Despite their best efforts, the police couldn't catch him, Filan. Further Filan sold his services online with each successful swatting call Filan felt more untouchable so he wanted to make money from his skills he created a telegram Channel called tour swats offering his swatting services for hire for \$40 he would report a fire or gas leak he charged \$50 for a major police response, and for \$75 he would report something much worse. Filan even offered returning customers a discount to attract more customers he made posts bragging about his swatting skills in a post in January 2023 Filan claimed that when he swats someone he usually gets the cops to drag the victim and their families out of the house, cuffed and searched the house for bodies Filan didn't care that his actions could ruin lives he was planning to do it hundreds more times for nearly 2 years Filan stayed one step ahead of the law To discover his identity the FBI launched a National Database to track swatting calls helping hundreds of police departments share information they also monitored the telegram Channel where he sold his swatting services and linked it to his usernames on YouTube and Discord. Eventually, the trail led straight to Filan's home in Lancaster, California, in January 2024. The police raided Filan's home and found electronic devices loaded with evidence, chat logs, recordings, and everything they needed to prove he was behind the swatting spree. It might have caused danger to somebody's life one day.

Table: Alan Filan Case Study Chart (Self-Created)

Acts	<ol style="list-style-type: none"> 1. Made 375+ fake 911 calls (“swatting”) nationwide. 2. Targeted: private homes, schools, churches, military bases, even FBI agents & U.S. senators, 3. Used caller ID spoofing & text-to-speech software to hide identity 4. Created a Telegram channel offering “swatting-for-hire” services: \$40 – fire/gas leak \$50 – major police response \$75 – severe/violent threats 5. Posted online bragging about his “skills” and discounted repeat services
Impact	<ol style="list-style-type: none"> 1. SWAT raids on innocent people’s homes 2. Risk of injury or death to victims & police officers 3. Waste of substantial law enforcement resources across states
Primary offences:	<ol style="list-style-type: none"> 1. <i>18 U.S.C. § 1038</i> – False information & hoaxes 2. <i>18 U.S.C. § 875(c)</i> – Interstate threats 3. <i>18 U.S.C. § 1028A</i> – Identity theft 4. State-level “false emergency reporting” laws

The USA Court recognized the **gravity of the offence** and the **public danger** this case has caused. The Judge acknowledged the

developmental immaturity of the accused but stressed **deterrence**, given the scale of acts deviating from the principles of the UNCRC. The



Hon'ble Court transferred the case to the adult court based on the repetitive nature of the offence, Cross-state federal crimes, and commercial motive. Filan was sentenced to several years in a federal juvenile detention center, probation until age 21, mandatory counselling, internet restrictions, and community service.

Both these cases highlight High technical skill at a young age and a Lack of proportional juvenile response systems. It is to be seriously considered that Swatting is not a prank; it is potentially lethal and causes tremendous security concerns. Digital offences by minors require a targeted federal policy to balance rehabilitation & deterrence.

Key Takeaways for India

1. U.S. courts may **transfer juveniles to adult jurisdiction** in extreme cyber cases involving repeated, profit-driven, and interstate impact
2. Indian JJ Act's **Section 15 preliminary assessment** has parallels but lacks:
 - a. Detailed cyber-risk evaluation methods
 - b. Federal-level specialized cyber juvenile prosecutors
3. U.S. sentencing incorporated rehabilitation conditions and tech-use monitoring, which can be considered modern punitive and rehabilitative initiatives that Indian courts could adopt instead of the current trend. This will be highlighted with the case study mentioned below.

Case Study: Trial of a Juvenile as an Adult in a Cybercrime—A Critical Appraisal Through the Lens of Hacked (2020)

Factual Matrix: In a hypothetical scenario inspired by the events portrayed in the film *Hacked* (2020), a 17-year-old male individual ("X"), technologically proficient and academically sound, becomes involved in a personal dispute with an adult female ("Y"), a professional working in the publishing industry. Upon facing emotional rejection, X proceeds to engage in unauthorized access to Y's personal digital devices, extracts sensitive information, including private photographs and correspondence, and subsequently circulates the same via online platforms and fabricated news outlets. The acts result in grave emotional distress and reputational damage to Y, affecting her personal and professional life.

Analytical build-up:

Upon filing of an FIR under Sections 66E, 67, and 72 of the Information Technology Act, 2000, read with Section 354D of the Indian Penal Code (IPC), the cyber cell identifies X as the primary accused. Considering the nature of the offense and its psychological impact on the survivor, the Juvenile Justice Board conducts a preliminary assessment under Section 15 of the Juvenile Justice (Care and Protection of Children) Act, 2015, to evaluate whether X should be tried as an adult.

Legal Issue:

Whether a 17-year-old individual accused of cybercrime involving mental harassment, digital voyeurism, and reputational assault should be tried as an adult under Section 15 read with Section 18(3) of the Juvenile Justice Act, and whether such a trial structure is consistent with the evolving principles of juvenile justice in India and international standards.

Arguments and Legal Analysis

1. Inconsistency with the Principle of 'Best Interest of the Child': The *UN Convention on the Rights of the Child (1989)*, ratified by India, mandates that children under 18 years must not be subjected to adult judicial processes, especially in criminal trials. Article 40 emphasizes rehabilitation and reintegration over punitive measures. Trying a juvenile as an adult contradicts this norm and risks infringing upon India's treaty obligations.
2. Discretionary, Arbitrary Nature of Preliminary Assessment: Section 15 of the JJ Act allows for a "preliminary assessment" of mental and physical capacity, understanding of consequences, and circumstances of the offense. However, such assessments are inherently subjective and lack statutory clarity. They are often conducted without the involvement of trained psychologists or forensic experts. This leads to an arbitrary determination of whether a juvenile offender possesses the "mens rea" comparable to an adult, particularly problematic in nuanced cybercrime cases that involve digital skills but not necessarily criminal intent.
3. Failure to Recognize the Distinct Psychology of Digital Offenders: Juveniles engaged in cybercrimes often operate in virtual spaces divorced from physical and emotional consequences.



Their actions may not stem from violent or malicious predispositions but from immature perceptions of power, validation, or retaliation. In the hypothetical case, X's actions, while gravely damaging, appear emotionally driven and reflect poor impulse control rather than calculated criminality.

4. Lack of Institutional Readiness for Adolescent Cyber Offenders
Indian law enforcement, judicial institutions, and rehabilitation facilities are yet to develop digital literacy protocols or reform-oriented correctional models tailored for adolescent cyber offenders. Trying X as an adult not only subjects him to the rigors of the criminal justice system but also exposes him to incarceration in environments unsuitable for reform.
5. Contradiction with the Objective of the JJ Act: The stated objective of the JJ Act, as found in its Preamble and Statement of Objects and Reasons, is to ensure care, protection, and rehabilitation of children in conflict with law. By permitting adult trials for children aged 16–18 based on a preliminary assessment, the law undermines its rehabilitative foundation and adopts a retributive posture incompatible with juvenile justice jurisprudence.
6. Comparative Jurisprudence: In *Roper v. Simmons*, 543 U.S. 551 (2005), the U.S. Supreme Court held that imposing adult criminal penalties on juveniles is unconstitutional due to the neurobiological differences in adolescent development. Similarly, in *UN General Comment No. 10 (2007)*, the Committee on the Rights of the Child emphasized that children's diminished capacity must be a cornerstone of juvenile justice systems.

Avenues for Change: Possible Solutions for India

The Tackling of core issues becomes imperatively unignorable; justice in India is always drawn from the letters of law. The party that wins the case gets its justice. It's never about who is right and wrong. First and foremost, the solution is that the legislators amend the definition of child in such a way that there is no constitutional validity debate just on the definition clause. Applauding the state government and law enforcement authorities in publishing handbooks, guidelines, and various

other communicable works, such as the Ministry of Home Affairs publishing booklet (2018) to safeguard the children against cyber threats, it still lacks enforceable awareness and implementation. The publications made by respective institutions should be backed by community-based support and localized youth-based groups to realize the fruits of knowledge.

Against the subjective preliminary assessment, there shall be substantial investment in research and development, to which further the government should be able to generate human capital in such a way that it has the capacity to deliver strengthened evidence. Because the author believes that the preliminary assessment has legitimacy when it is developed in the requirement of a more organised patient, clinical, educational, statistical, and informatics infrastructure for trials and evaluation.

In social reform. advocating and promoting rehabilitative approaches by decriminalizing minor misbehaviours and focusing on restorative interventions to prevent unnecessary entry of children into the criminal justice system, and developing their current unique skills would reward both the individual and the state.

For heinous offences, Reports and court orders should indicate a shift towards accountability, even for technically savvy minors. Again, the state must take up the doctrine of *parens patriae* and rehabilitate as well as reform these individuals so that they are helpful to themselves and the state.

Create child-friendly spaces in police stations, train officers in trauma-sensitive and child-centered communication, for both victims and minor offenders. Indian Prototype that already in effect is Mumbai's new "Matunga model" stations include safe corners with toys, books, and calming décor, supporting minors in crisis and easing their interaction with law enforcement. This promotes early engagement in child child-friendly manner, facilitating the best interest of the child. Lastly, according to *The Daily Telegraph* (n.d.), taking a page from Spain's *Diagrama Model* that strengthened itself with re-education centers staffed by educators, social workers, psychologists, and very few security personnel, this allowed 84% of youth to reintegrate without reoffending—Australia is now adapting this model as well.

Conclusion

In India, when a juvenile is accused of committing a cybercrime, exclusive jurisdiction lies with the



Juvenile Justice Board, unless a preliminary assessment under Section 15 justifies a transfer to the Children’s Court. Territorial jurisdiction follows standard criminal procedure rules, but is influenced by the location of the offence, the accused, and the victim. While the legal framework is clear, practical challenges persist due to the lack of technical expertise within juvenile adjudicatory bodies to handle sophisticated cyber offences. Further, the fictional case highlights a fundamental legal paradox: a minor possessing sufficient technological knowledge to commit cybercrime may still lack the emotional and psychological maturity to comprehend its full implications. Permitting the trial of 16–18-year-olds as adults in such cases may satisfy retributive urges but ultimately fails both the offender and the justice system. India’s legislative framework must be reoriented to integrate restorative digital justice models, strengthen psychological assessment protocols,

and prioritize rehabilitation over punishment in dealing with adolescent cyber offenders.

Technology is merely a tool, a physical capital its use good or bad or heinous nature will always depend on the user. A child, a minor, or a juvenile, irrespective of the nomenclature, faces the same infinite potential pool of danger, and society can never do away with the children or the technology. In a comparative dimension, the study examines juvenile justice frameworks across various democratic jurisdictions to identify best practices and reformative approaches that may inform the Indian context.

The paper ultimately seeks to reconcile the statutory objective of juvenile justice with its foundational principles—rehabilitation, reintegration, and the paramountcy of the best interests of the child—while proposing constructive policy recommendations to bridge existing normative and practical gaps.

References

- Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2, Acts of Parliament, 2016 (India).
- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- Adusumilli, S. (2024, December). The evolution of juvenile justice jurisprudence in India: Retribution to restoration. *White Black Legal – The Law Journal*, 3(1). <https://www.whiteblacklegal.co.in>
- ICLG. (2024, November 6). *Cybersecurity laws and regulations: India 2025. International Comparative Legal Guides*. <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india>
- Anand, M. (2023). Cybercrime and cyber laws in India. *Indian Journal of Law and Legal Research*, 5(2). <https://heinonline.org/HOL/LandingPage?handle=hein.journals/injllw11&div=224&id=&page=>
- Mack, J. W. (1909). The juvenile court. *Harvard Law Review*, 24(2), 104–122.
- Nieborg, S., Verwey-Jonker Instituut, & others. (2000). *Child and juvenile delinquency: Strategies of prevention and intervention in Germany and the Netherlands* (p. 20). Verwey-Jonker Instituut.
- Pickles, A., Edwards, D., Horvath, L., & Emsley, R. (2023). Research reviews: Advances in methods for evaluating child and adolescent mental health interventions. *Journal of Child Psychology and Psychiatry*, 64(12), 1765–1775. <https://doi.org/10.1111/jcpp.13892>
- Johnson, S. B., Blum, R. W., & Giedd, J. N. (2009). Adolescent maturity and the brain: The promise and pitfalls of neuroscience research in adolescent health policy. *Journal of Adolescent Health*, 45(3), 216–221. <https://doi.org/10.1016/j.jadohealth.2009.05.016>
- Singh, D. (2019). An analysis of Section 15 of the Juvenile Justice Act, 2015. *Christ University Law Journal*, 8(2), 1–23. <https://doi.org/10.12728/culj.15.1>
- Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: Trends and challenges. *International Journal of Innovations & Advancement in Computer Science*, 6(12), 187–195.
- Retrieved from https://www.researchgate.net/profile/Jun-ee-Iqbal/publication/322245372_Cybercrime_in_India_Trends_and_Challenges/links/5a4e040c458515a6bc6ea9e3/Cybercrime-in-India-Trends-and-Challenges.pdf
- Khan, N., & Gulati, S. (2023). International legislative framework of cybercrimes: A comparative study of India, Israel, and USA. *Journal of Positive School Psychology*, 7(1), 782–800. <http://journalppw.com>
- Bhatia, V. (Director). (2020). *Hacked* [Film]. Loneranger Productions; Zee Studios.



- Roper v. Simmons, 543 U.S. 551 (2005): Supreme Court of the United States. (2005). *Roper v. Simmons*, 543 U.S. 551.
- Supreme Court of India. (2014, March 28). *Dr. Subramanian Swamy & others v. Raju through Member, Juvenile Justice Board & another*, SLP (CrI.) No. 1953 of 2013. <https://indiankanoon.org/doc/134314390/>
- Supreme Court of India. (2017). *Mukesh & another v. State for NCT of Delhi & others*, (2017) 6 SCC 1. <https://indiankanoon.org/doc/31205809/>
- Venkatesan, J. (2021, November 16). *SC reserves orders on validity of Juvenile Justice Act: 'The Act provides for a straitjacket interpretation of 'juvenile:' a person below 18 is a minor'*. *The Hindu*. <https://www.thehindu.com/news/national/sc-reserves-orders-on-validity-of-juvenilejustice-act/article5631810.ece>
- United Nations. (1985). *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (The Beijing Rules)*. <https://www.ohchr.org/en/instruments-mechanisms/instruments/united-nations-standard-minimum-rules-administration-juvenile>
- The Daily Telegraph. (n.d.). *Youth crime prevention: Spanish program that could help Australia's troubled youth*. The Daily Telegraph. https://www.dailytelegraph.com.au/subscribe/news/1/?sourceCode=DTWEB_WRE170_a&dest=https%3A%2F%2Fwww.dailytelegraph.com.au%2Ftruecrimeaustralia%2Fyouth-crime-prevention-spanish-program-that-could-help-australias-troubled-youth%2Fnews-story%2F87bba05907ec8f8b29ad6bf8df348499&memtype=anonymous&mode=premium&v21=GROUPA-Segment-1-NOSCORE
- United Nations. (1989). *Convention on the Rights of the Child*. <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>
- The Times of India. (2025, July 21). *Cyber-police arrest two men for financial fraud using fake Parivahan app*. *The Times of India*. Retrieved from Times of India website <https://timesofindia.indiatimes.com/city/kochi/cyber-police-arrest-two-men-for-financial-fraud-using-fake-parivahan-app/articleshow/122800585.cms>
- Constitution of India, 1950 (India). <https://legislative.gov.in/constitution-of>