Page 1624 - 1636

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Juvenile Delinquency and Cybercrime: Emerging Challenges in the Digital Age

DR. SURINDER KALYAN[*] AND ASHWINI KISHORI YADAV[**]

ABSTRACT

Digital technology has reordered the conditions of adolescence. It has widened access to learning, creativity and friendship, and it has at the same time made juvenile delinquency a substantially harder phenomenon to define, detect and answer. This article offers a critical narrative review of the legal, sociological and policy literature on juvenile cyber-delinquency, centred on India but drawing on comparative material. Its central claim is that cyber-delinquency cannot be treated as ordinary adolescent mischief that happens to occur online. Young people move between victimisation, experimentation, status-seeking and offending within the same digital environments, often within a single episode. Platform architecture compounds the difficulty: perceived anonymity lowers inhibition, recommendation systems surface harmful material, and gaming, messaging, generative artificial intelligence and crime-as-a-service markets shorten the distance between curiosity and serious harm, while mediated interaction dulls the perception of wrongfulness. The institutional response remains fragmented. Substantive law addresses discrete offences rather than the ecosystem that produces them; schools rely on episodic awareness activity; parental understanding of children's online lives is limited; and juvenile justice institutions lack digital-forensic and mental-health expertise. The article argues for a reorientation that places the child at the centre and pairs accountability with early help, safety-by-design obligations on intermediaries, specialist investigative capacity, mental-health provision, restorative options and legitimate pathways into ethical cybersecurity practice. It proposes a layered model integrating digital literacy, youth wellbeing and cybersecurity into a juvenile justice system fit for a networked society.

Keywords: *juvenile cyber-delinquency, cybercrime, social media, artificial intelligence, juvenile justice, rehabilitation, India*

I. INTRODUCTION

The context and meaning of adolescent deviance have altered with the rise of networked life. Within a single hour a mobile handset may serve as a classroom, a social arena, a gaming console, a marketplace and an instrument of harm. Conduct that once required physical

[*] Author is an Associate Professor at NIILM University, Kaithal, Haryana, India.
[**] Author is a Research Scholar at NIILM University, Kaithal, Haryana, India.

 [ISSN 2581-5369]

proximity, such as bullying, intimidation, theft, sexual harassment or reputational injury, can now be repeated, automated and distributed to an almost unlimited audience.[1] Other conduct, including the deployment of malware, unauthorised access and distributed denial-of-service attacks, depends upon digital systems for its very existence.[2] The result is not merely a new catalogue of offences. It is an altered opportunity structure in which low cost, perceived anonymity, rapid peer feedback and weak adult visibility compress the distance between curiosity and consequential harm.

Recent scholarship describes juveniles as at once vulnerable users and capable actors. Prolonged and unsupervised exposure to violent or deviant digital content has been associated with cyberbullying, breach of privacy and social withdrawal, although the direction of causation is rarely established.[3] Work on the Indian legal system has additionally emphasised peer pressure, the routine normalisation of copyright infringement among young users, and the practical inability of platforms to distinguish child users from adult users, with the consequence that material and contacts calibrated for adults reach children as a matter of course.[4] More recent work identifies social onboarding through games and messaging services, the ready availability of attack tools, and status-based online communities as routes towards more serious conduct.[5] The evidence base nevertheless remains patchy. Local surveys, interviews conducted in observation homes, doctrinal legal analysis and policy briefs answer different questions and ought not to be conflated into a single prevalence estimate.

This article is a critical narrative review of that literature. Its central argument is that juvenile cyber-delinquency emerges from the interaction of developmental vulnerability, social reinforcement, technological affordance and institutional gaps. Effective policy must therefore reach beyond increased punishment or restricted access. It should interrupt escalation, repair harm, build competent guardianship and redirect technical competence towards legitimate participation.

II. Conceptualising Juvenile Cyber-Delinquency

Juvenile delinquency has conventionally been defined as unlawful conduct by a person below the age fixed by the relevant jurisdiction. In India the Juvenile Justice (Care and Protection of

[1] Stefan Tiberiu Ciurea, *Juvenile Delinquency and the Online Environment: A New Challenge to Society*, 21(2) Acta Universitatis Danubius. Juridica 86 (2025).
[2] Zino Haro, *The Rise of Youth Cybercrime: Social Trends and Interventions*, New America (Oct. 21, 2025).
[3] Ciurea, *supra* note 1, at 88-90.
[4] Astha Srivastava & Shivangi Sinha, *Cyber Delinquency: Issues and Challenges Under Indian Legal System*, 8(5C) International Journal of Engineering and Advanced Technology (May 2019).
[5] Haro, *supra* note 2.

 [ISSN 2581-5369]

Children) Act, 2015 defines a child as a person who has not completed eighteen years of age, and a child in conflict with law as a child alleged or found to have committed an offence who had not completed eighteen years on the date of its commission.[6] The term 'cybercrime', by contrast, describes a heterogeneous set of behaviours. It is useful to distinguish cyber-enabled offences, being traditional harms facilitated by technology such as fraud, stalking, extortion and identity theft, from cyber-dependent offences, which could not exist without computer systems, such as malware distribution, botnet operation and unauthorised network intrusion.[7] Indian law tracks this division imperfectly but recognisably. Cheating, cheating by personation, forgery and criminal intimidation are addressed by the general criminal law now contained in the Bharatiya Nyaya Sanhita, 2023,[8] whereas dishonest or fraudulent interference with a computer resource, identity theft, cheating by personation using a computer resource and violation of bodily privacy are addressed by ss. 66, 66C, 66D and 66E of the Information Technology Act, 2000.[9] A second distinction matters equally for juvenile justice: harmful digital behaviour is not always criminal, while conduct that is technically criminal spans a wide range of intent, sophistication and harm.

Adolescents may be victims, witnesses, coerced participants and offenders at different moments within a single episode. A young person groomed in a gaming community may share credentials, perform a small task for an older actor and eventually recruit peers.[10] An individual subjected to image-based abuse may in turn retaliate by compromising an account or redistributing material without consent, conduct that is itself an offence under ss. 66E and 67A of the Information Technology Act, 2000 and, where the person depicted is a child, under the Protection of Children from Sexual Offences Act, 2012 and s. 67B of the Information Technology Act.[11] Binary labels obscure coercion, developmental immaturity and the social processes by which behaviour escalates. A child-centred assessment should therefore examine intent, knowledge, role, benefit, coercion, repetition, technical capability and harm, and not merely the digital footprint left behind.

The boundary between experimentation and delinquency is especially difficult to draw online. Copying code, probing a system or modifying a game may be framed as play or as technical

[6] The Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2 of 2016, ss. 2(12), 2(13) (India).
[7] Haro, *supra* note 2 (distinguishing cyber-enabled from cyber-dependent offending).
[8] The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, ss. 318, 319, 336, 351 (India).
[9] The Information Technology Act, 2000, No. 21 of 2000, ss. 66, 66C, 66D, 66E (India). Section 66 punishes the dishonest or fraudulent commission of any act referred to in s. 43 with imprisonment up to three years or fine up to five lakh rupees, or both.
[10] Haro, *supra* note 2 (social onboarding through gaming platforms and messaging services).
[11] The Information Technology Act, 2000, ss. 66E, 67A, 67B (India); The Protection of Children from Sexual Offences Act, 2012, No. 32 of 2012, ss. 13, 14, 15 (India).

 [ISSN 2581-5369]

learning, yet becomes unlawful where consent and authorisation are absent. Section 43 of the Information Technology Act, 2000 attaches liability to access secured without the permission of the owner or person in charge, and s. 66 converts the same conduct into a punishable offence where it is done dishonestly or fraudulently.[12] Digital acts also appear reversible when their consequences are not. Data persist, duplicate and resurface; victims can be contacted repeatedly; and a single ill-advised post may reach an audience far larger than the juvenile anticipated. These features strengthen the case for early ethical education and proportionate diversion, rather than for deferring intervention until conduct has become gravely harmful.

A socio-technical perspective further shows that an account resting on individual pathology is only partial. Platforms determine what conduct is visible, rewarded and easy to reproduce; families and schools supply guardianship; peer groups supply norms; and markets supply incentives.[13] Moral disengagement may occur where the target is represented only as an account, an avatar or an institution, where responsibility is diffused across a group, or where harm is described as a prank, a challenge or a victimless test. These mechanisms do not excuse conduct, but they identify points of intervention. Ethical prompts, visible consent boundaries, rate limits, peer-bystander training and immediate feedback on real-world impact can disrupt the cognitive distance that digital interfaces create.

III. The Structure of Risk

Developmental factors create susceptibility, not destiny. Adolescents tend to weigh peer approval, novelty and immediate reward more heavily than adults do, and are still developing impulse control and long-term risk assessment. Online environments amplify these tendencies by rendering status measurable in followers, ranks, reactions and access to exclusive groups. Ciurea identifies prolonged exposure to violent or deviant digital content, the absence of parental supervision and group influence as the principal contextual correlates of online delinquency among minors.[14] Haro goes further, identifying belonging and prestige as central motivations along many pathways into youth cybercrime and reporting that the great majority of young offenders act not from ideology or organised sponsorship but from boredom, peer status-seeking and modest financial incentive.[15] Technical success can serve as a visible demonstration of competence in settings where legitimate recognition is scarce.

[12] The Information Technology Act, 2000, ss. 43, 66 (India).
[13] Ciurea, *supra* note 1, at 90-93; Haro, *supra* note 2.
[14] Ciurea, *supra* note 1, at 89-92.
[15] Haro, *supra* note 2 (reporting that in eighty to ninety per cent of cases young offenders are not motivated by ideology or organised sponsorship, and that belonging is a central motivation in fifty-five to seventy-five per cent of cases).

 [ISSN 2581-5369]

Social media, gaming and encrypted messaging environments also collapse recruitment, instruction and offending into a single space. Tutorials, stolen credentials, target lists and peer encouragement circulate alongside ordinary conversation.[16] Adolescents need not seek out a stereotypical 'dark web' marketplace; entry points are found in mainstream communities and migrate gradually to less visible channels. This normalisation lowers moral barriers by fragmenting the task. One participant supplies access, another automates messages, another monetises data, and each can disclaim personal responsibility.

Crime-as-a-service and generative artificial intelligence have made that progression more accessible still. Generative systems can produce plausible phishing text, translate scams across languages, synthesise images or voices and assist with code, while capabilities that formerly demanded expertise are now packaged in subscription toolkits.[17] Such developments do not eliminate the need for skill, but they reduce the cost of entry and accelerate the learning curve. They also complicate attribution, since investigators must distinguish original authors from tool operators, coerced intermediaries and juveniles who imitate demonstrations without comprehending scale. Artificially generated sexual or humiliating content creates a further harm vector, because fabrication can be rapid, personalised and difficult to remove. Indian law has begun to respond: r. 3(2)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 requires an intermediary to remove or disable access, within twenty-four hours of a complaint, to material exposing an individual's private area, depicting nudity or a sexual act, or artificially morphed to suggest either.[18]

Structural conditions also matter. Digital exclusion and digital risk are linked. Children from economically disadvantaged backgrounds may turn to illicit income, whereas those from more privileged backgrounds often enjoy greater device access and more advanced technical skill. The mixed-method study conducted by Misra and Tiwari with juveniles apprehended at the Lucknow observation home records stakeholder perceptions across income groups rather than a single class profile.[19] Explanations resting on poverty alone are therefore insufficient. Risk is better conceived as a combination of access, strain, opportunity, supervision and attachment to online groups.

---

[16] Haro, *supra* note 2.

[17] Haro, *supra* note 2 (on the commodification of hacking tools through malware-as-a-service platforms and the lowering of entry barriers by artificial intelligence).

[18] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b) (India).

[19] Pawan Kumar Misra & Saurabh Tiwari, *Cyber-Delinquency and Its Impact on Children's Mental Health: Legal Challenges in India*, 12(12) INTERNATIONAL JOURNAL OF RESEARCH AND SCIENTIFIC INNOVATION 1588 (2025), doi:10.51244/IJRSI.2025.12120135.

 [ISSN 2581-5369]

Family supervision must further be distinguished from invasive surveillance. Covert reading of all messages may inhibit openness, drive communication to concealed accounts and erode trust. Effective guardianship is relational: carers set age-appropriate boundaries, model secure behaviour, understand the child's online communities and respond calmly when difficulties arise.[20] Schools can support this by treating online incidents as safeguarding and learning matters rather than as simple disciplinary breaches. Conflicts travel from classroom to platform and back again, so institutional responsibility should turn not on where the first message was sent but on the foreseeable consequences for student safety.

IV. Forms and Consequences of Juvenile Cybercrime

Juvenile online offending ranges from interpersonal aggression to technically sophisticated and financially motivated conduct. Cyberbullying, impersonation, stalking, doxxing and non-consensual image sharing exploit the persistence and reach of platforms. Fraud takes the form of account takeover, money-mule activity, payment deception and phishing. Digital piracy and credential sharing are frequently normalised as low-harm behaviour. At the technical end lie unauthorised access, malware, botnets and service disruption. Indian law distributes these across several instruments: stalking, obscenity, cheating, cheating by personation, forgery and criminal intimidation under the Bharatiya Nyaya Sanhita, 2023, and computer-related offences, identity theft, personation by computer resource, violation of privacy and the publication or transmission of obscene, sexually explicit or child sexual abuse material under the Information Technology Act, 2000.[21] Table 1 classifies these forms by mechanism and by intervention need.

The consequences extend well beyond formal legal liability. Victims may experience fear, shame, disrupted sleep, anxiety, school avoidance and lasting reputational damage. For young offenders, arrest or public exposure can interrupt education, strain family relationships and fix a durable deviant label. Empirical work with juveniles in the Lucknow observation home links compulsive internet use, isolation and exposure to harmful content to mental-health concerns, though causal claims drawn from a single-site mixed-method study should be treated with caution.[22] The wider literature likewise records psychological distress and loss of control over personal information among young people affected by cybercrime, but the strength of that association rests largely on small and self-selected samples and is not yet established at population level.

[20] Ciurea, *supra* note 1, at 91.
[21] The Bharatiya Nyaya Sanhita, 2023, ss. 78, 294, 295, 318, 319, 336, 351 (India); The Information Technology Act, 2000, ss. 66, 66C, 66D, 66E, 67, 67A, 67B (India).
[22] Misra & Tiwari, *supra* note 19.

 [ISSN 2581-5369]

Purely punitive responses are particularly hazardous because of the overlap between victim and offender. A juvenile subjected to grooming, coercion or threats from peers may require safeguarding even while being held to account. Conversely, treating all such conduct as harmless experimentation minimises serious victim impact. The Juvenile Justice (Care and Protection of Children) Act, 2015 already contemplates a graduated response, its general principles governing the administration of the Act and s. 18(1) offering the Board a range of dispositions from advice and admonition, group counselling and community service through to release on probation and, in the last resort, placement in a special home.[23] A calibrated response should acknowledge harm, require repair where repair is possible, and avoid sanctions that deepen isolation or place inexperienced young people in contact with more entrenched offenders.

Harm and visibility are also shaped by gender and social location. Girls and sexual-minority youth appear to be disproportionately targeted with sexualised harassment, image-based abuse and threats of exposure. Boys may be more readily recruited into status-oriented technical groups and may be less likely to disclose victimisation. Children with disabilities, limited literacy or weak support networks face additional barriers to reporting. These observations, which rest on practitioner accounts rather than on representative Indian data, should inform the design of accessible services without hardening into stereotypes about who is victim and who is offender. Assessment must remain individualised and must recognise that shame, fear of device confiscation and anticipated blame suppress disclosure across all groups.

Table 1. Typology of juvenile cyber-delinquency and implications for intervention

Interpersonal aggression. Typical conduct and digital mechanism: cyberbullying, stalking, doxxing, impersonation. Principal risks: repeated victimisation, reputational and psychological harm. Priority response: safety planning, content action, counselling, restorative option.

Sexual and image-based harm. Typical conduct and digital mechanism: coercive sharing, synthetic imagery, non-consensual sharing. Principal risks: trauma, extortion, permanent recirculation. Priority response: immediate safeguarding, specialist investigation, victim-led removal.

Identity and financial abuse. Typical conduct and digital mechanism: phishing, account takeover, payment fraud, money-mule tasks. Principal risks: financial loss, organised recruitment, escalation. Priority response: trace roles and coercion, restitution, targeted diversion.

[23] The Juvenile Justice (Care and Protection of Children) Act, 2015, ss. 3, 18(1) (India).

 [ISSN 2581-5369]

Content and access offences. Typical conduct and digital mechanism: piracy, credential sharing, unauthorised access. Principal risks: normalisation of illegality, damage to systems. Priority response: ethics education, supervised technical pathway, proportionate sanction.

Cyber-dependent attacks. Typical conduct and digital mechanism: malware, botnets, distributed denial-of-service, automated intrusion. Principal risks: large-scale disruption, cross-border evidence problems. Priority response: specialist forensics, role differentiation, structured rehabilitation.

Source: authors' synthesis of the literature reviewed.

V. Legal and Institutional Barriers

India's response rests on the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, the general criminal law now contained in the Bharatiya Nyaya Sanhita, 2023, and the Juvenile Justice (Care and Protection of Children) Act, 2015.[24] A data-protection layer has recently been added by s. 9 of the Digital Personal Data Protection Act, 2023, which requires a data fiduciary to obtain verifiable parental consent before processing the personal data of a child, forbids processing likely to have a detrimental effect on a child's well-being, and prohibits tracking, behavioural monitoring and targeted advertising directed at children.[25] That layer is largely untested in practice and is subject to exemption by notification.

The rehabilitative orientation of the juvenile framework is normatively appropriate to developmental immaturity. The Act graduates its response by seriousness, distinguishing petty offences, serious offences and heinous offences, the last being those for which the law prescribes a minimum punishment of imprisonment for seven years or more, and requiring the Juvenile Justice Board to conduct a preliminary assessment of mental and physical capacity, ability to understand consequences and surrounding circumstances where a child who has completed sixteen years is alleged to have committed a heinous offence, with a consequent order under s. 18(3).[26] The 2021 amendment closed a gap by bringing within 'serious offences' those offences carrying a maximum of more than seven years where no minimum, or a minimum of less than seven years, is provided.[27] Cyber cases nevertheless expose coordination problems. Srivastava and Sinha underline the absence of a simple, offence-specific juvenile cyber

[24] The Information Technology Act, 2000 (India); The Protection of Children from Sexual Offences Act, 2012 (India); The Bharatiya Nyaya Sanhita, 2023 (India); The Juvenile Justice (Care and Protection of Children) Act, 2015 (India).
[25] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, s. 9 (India).
[26] The Juvenile Justice (Care and Protection of Children) Act, 2015, ss. 2(33), 2(45), 2(54), 15, 18(3) (India).
[27] The Juvenile Justice (Care and Protection of Children) Amendment Act, 2021, No. 23 of 2021 (India) (in force 1 September 2022).

 [ISSN 2581-5369]

regime.[28] Independent assessment of the institutional base is sobering: across the child care institutions surveyed for the INDIA JUSTICE REPORT, only twenty-eight medical officers were in post for one hundred and twenty-eight institutions, close to eighty per cent of institutions reported no doctor at all, and of the two hundred and ninety-two districts returning usable data only eleven met the basic minimum conditions the Act contemplates.[29] Misra and Tiwari accordingly argue for closer integration of cyber, child-protection and juvenile-justice mechanisms.[30]

Four operational gaps recur. First, jurisdiction and evidence are dispersed across devices, platforms and borders, while delay can erase logs or permit further dissemination. Second, generalist police, probation staff, counsellors and Board members may lack a shared vocabulary for describing technical conduct and developmental capacity, notwithstanding that the Board is constituted with a Metropolitan or Judicial Magistrate and two social workers precisely in order to combine legal and welfare expertise.[31] Third, children often find platform reporting and removal systems difficult to navigate. Fourth, legal categories capture graded participation in group activity poorly. A single event may involve an adult organiser, a juvenile coder, a coerced account holder and a school peer who forwards content.

Procedural justice therefore requires close attention. The confiscation of a device can expose sensitive personal information unrelated to the allegation; school discipline may be imposed without reliable attribution; automated detection generates false positives; and broad monitoring threatens privacy. The Act itself prohibits any report that discloses the name, address, school or other particulars capable of identifying a child in conflict with law or a child victim or witness.[32] Child protection cannot be equated with continuous surveillance, and any interference with privacy must satisfy the tests of legality, necessity and proportionality laid down by the Supreme Court.[33] Investigations must accordingly be lawful, necessary and proportionate, conducted with age-appropriate explanation, with access to counsel or guardians where required, and with careful handling of child sexual abuse material. Diversion decisions should turn on technical and psychosocial assessment rather than on the offence label alone.

Digital evidence presents a further problem of interpretation. Possession of a tool does not establish its use; an internet protocol address does not identify a user; and presence in a channel

[28] Srivastava & Sinha, *supra* note 4.
[29] INDIA JUSTICE REPORT, *Juvenile Justice and Children in Conflict with the Law* (2025).
[30] Misra & Tiwari, *supra* note 19.
[31] The Juvenile Justice (Care and Protection of Children) Act, 2015, ss. 4, 8 (India).
[32] *Id.* s. 74.
[33] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

 [ISSN 2581-5369]

does not signify agreement with everything said there. Deletion may indicate panic rather than sophisticated concealment. Investigators need timelines that combine technical artefacts with interviews, school and family context, benefit flows and evidence of instruction or coercion. The evidentiary framework reinforces this discipline, since s. 63 of the Bharatiya Sakshya Adhiniyam, 2023 admits an electronic record only on satisfaction of the statutory conditions and on production of a certificate signed both by the person in charge of the device and by an expert.[34] A written role assessment reduces the risk that the most technically visible child is made to answer for a network operated by adults. The same discipline benefits victims, since better attribution avoids premature accusation and the lasting harm it causes.

VI. A Unified Prevention and Response Framework

Prevention must be layered. Schools and platforms require universal measures: practical digital ethics, consent, password security, recognition of scams, bystander action and clear routes to reporting. Such education should inform rather than rely on admonitory slogans, and should draw a clear line between legitimate security research and unauthorised access. Parents require brief, usable guidance on supportive supervision rather than screen-time limitation alone. Schools should adopt predictable response protocols that preserve evidence, protect victims and avoid public shaming.

Targeted intervention should follow early warning signs such as repeated account misuse, participation in harmful groups, unexplained digital income, compulsive use or escalating online conflict. A multidisciplinary team can assess safety, mental health, coercion, family circumstances and technical conduct together. Where victims consent and power imbalances are manageable, restorative approaches may be appropriate. Agreements can include apology, efforts at removal, restitution, restricted access to specified systems, counselling and supervised learning.

Serious or repeated conduct requires specialised investigation and structured rehabilitation. Accountability may include judicial oversight, but detention cannot be the default answer to what is in substance a problem of digital skill and social belonging. Programmes should combine cognitive-behavioural work, family engagement, continuity of education, victim awareness and ethical cybersecurity training. Haro emphasises interventions that pair accountability with mentorship and legitimate technical pathways.[35] Such redirection is not leniency. It reduces recidivism by supplying a credible alternative to illicit status and belonging.

[34] The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63 (India).
[35] Haro, *supra* note 2.

 [ISSN 2581-5369]

Platforms and technology companies bear a distinct set of responsibilities. Safety-by-design measures can make harmful groups harder to discover, limit unsolicited contact from adults, slow mass forwarding, provide child-readable warnings, retain report status and accelerate the removal of intimate or exploitative material, an obligation already given statutory shape in the twenty-four-hour takedown requirement for non-consensual intimate imagery.[36] Risk assessments should examine the extent to which recommendation systems, monetisation and engagement incentives expose young people to offending communities, a question now sharpened by the statutory prohibition on tracking, behavioural monitoring and targeted advertising directed at children.[37] Transparency reports should carry child-specific indicators while withholding operational detail that would facilitate evasion.

Three predictable failures must be avoided in implementation. First, awareness campaigns become ritual where students cannot access confidential help after disclosure. Second, skills programmes may teach offensive techniques without consent, containment and ethical supervision. Third, multi-agency arrangements diffuse responsibility unless one professional is designated to coordinate the plan. Programmes should therefore state referral thresholds, response times, data-sharing limits and closure criteria. Supervised cyber ranges, capture-the-flag exercises and responsible-disclosure education can supply legitimate challenge, but access should be coupled with mentorship and explicit rules. Victim services must be available whether or not an offender is identified or prosecuted.

Table 2 allocates responsibility across institutions and Table 3 proposes outcome indicators. The organising principle is coordinated proportionality: the graver the harm and the stronger the intent, the more intensive the accountability; the greater the coercion, developmental limitation or welfare need, the stronger the safeguarding response.

Table 2. Multi-level allocation of responsibility for prevention

Family and caregivers. Core responsibility: supportive guardianship and early help-seeking. Illustrative measures: regular dialogue, privacy-aware supervision, discussion of scams and consent.

Schools. Core responsibility: universal prevention and incident response. Illustrative measures: scenario-based curriculum, designated reporting lead, evidence preservation protocol.

[36] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b) (India).
[37] The Digital Personal Data Protection Act, 2023, s. 9(3) (India).

 [ISSN 2581-5369]

Platforms. Core responsibility: safety-by-design and accessible remedy. Illustrative measures: child-readable reporting, friction on forwarding, rapid action on intimate content.

Police and juvenile justice. Core responsibility: child-sensitive and proportionate accountability. Illustrative measures: specialist triage, assessment of role and coercion, diversion with due process.

Health and social services. Core responsibility: meeting welfare and mental-health needs. Illustrative measures: trauma-informed care, family work, support for addiction and isolation.

Industry and civil society. Core responsibility: legitimate belonging and skills transfer. Illustrative measures: mentorship, cyber clubs, supervised laboratories, employability pathways.

Source: authors' synthesis of the literature reviewed.

Table 3. Indicators for assessing a child-focused cyber-delinquency strategy

Safety and victim recovery. Example measures: time to protection and removal; repeat contact; wellbeing and return to school. Why it matters: centres outcomes for the child rather than mere disposal of cases.

Proportionality and rights. Example measures: use of diversion; availability of legal assistance; minimisation of data unrelated to the allegation. Why it matters: tests fairness and privacy.

Rehabilitation. Example measures: retention in education; completion of counselling; participation in legitimate technical training. Why it matters: measures reintegration rather than punishment alone.

Recurrence. Example measures: repeat harmful behaviour at six, twelve and twenty-four months. Why it matters: demonstrates the durability of intervention.

Institutional capacity. Example measures: staff trained; speed of referral; cross-agency case coordination. Why it matters: identifies bottlenecks in implementation.

Platform accountability. Example measures: child reports resolved; time to response; appeal outcomes. Why it matters: links design and remedy to measurable duties.

Source: authors' synthesis of the literature reviewed.

VII. Research Agenda

Policy is constrained because the available data are not comparable. Police statistics record only incidents that are detected and reported, and the national series aggregates offences by legal

category rather than by the developmental profile of those involved.[38] School records employ divergent definitions, and platform data are proprietary. Local surveys illuminate attitudes but cannot demonstrate national prevalence. Future research should adopt consistent age bands, separate victimisation from perpetration, distinguish cyber-enabled from cyber-dependent conduct, and report gender, disability, location and socio-economic context without generating identifiable profiles.

Progression requires longitudinal testing. Which forms of experimentation desist spontaneously, what predicts escalation, and which interventions redirect technical skill without increasing contact with the criminal justice system? Evaluations should measure victim recovery, retention in education, recidivism, digital competence and family functioning, and not arrests alone. Young people should participate in designing prevention material and reporting systems, subject to ethical safeguards. Comparative work across jurisdictions can yield transferable principles, provided that differences in the age of criminal responsibility, in due process guarantees and in platform availability are held clearly in view.

VIII. Conclusion

Juvenile cyber-delinquency is an emergent governance challenge because it joins long-standing developmental and social pressures to technologies that amplify reach, speed, persistence and anonymity. Young people can move from victimisation to offending, and from low-level experimentation to organised harm, faster than conventional institutions can detect. Artificial intelligence and service-based criminal markets lower the barriers to entry further, while fragmented legal and welfare systems struggle to assign responsibility in proportionate terms.

A durable response must be child-centred without being indulgent. It should protect victims, respect due process, hold participants accountable in proportion to their conduct and prevent a youthful mistake from hardening into a criminal identity. Digital literacy, platform design, specialised investigation, mental-health support, restorative practice and legitimate cybersecurity pathways are not competing policies; they are components of a single prevention ecosystem. The central task for juvenile justice in the digital age is to convert technical ability and online belonging from risk factors into resources for law-abiding participation.

*****

[38] National Crime Records Bureau, *Crime in India 2023* (2025).

 [ISSN 2581-5369]