International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 10 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Juvenile Justice in the Digital Age: Legal Responses to Cybercrime, Online Grooming, and Children in Conflict with the Law

M.E. Rohan Sam Titus[1]
[1] Student, SRM SCHOOL OF LAW

***Abstract*—Children in India spend a great deal of their time online, and the law has not kept up. The article looks at how Indian law deals with three closely related issues: offences committed by children online, the grooming and exploitation of children by adults and the handling of digital evidence in cases involving a child. It contends that the framework is not absent, merely fragmented. The Juvenile Justice (Care and Protection of Children) Act, 2015; the Protection of Children from Sexual Offences (POCSO) Act, 2012; the Information Technology (IT) Act, 2000; the various criminal laws enacted in 2023; and the Digital Personal Data Protection Act, 2023 all deal with some aspect of the problem but were not designed to work in tandem. The article draws on the cases of *Shilpa Mittal* and *Just Rights for Children Alliance v. S. Harish* to illustrate the impact of this fragmentation on both child victims and children who are accused of offences, and makes a number of recommendations which would see rehabilitation, rather than punishment per se, at the heart of the response.**

***Index Terms*—Children in conflict with law, cybercrime, electronic evidence, juvenile justice, online grooming, POCSO Act, rehabilitation**

I. INTRODUCTION

A kid in India today is likely to encounter the world first on a screen. School, friends and fun all go via devices which many parents and teachers only have a very limited understanding of. That has dramatically increased access to learning but has also created new avenues for harm [1], [2]. Adults will use messaging apps and social media to gain a child's trust and then abuse that trust. The child may not even fully appreciate the ramifications and so will end up sharing private images, bullying their peers or passing on images of their peers that have been manipulated. The law has to protect the child who is harmed online and treat fairly the child who is the cause of the harm online and those two situations are often one and the same and on the same device.

This article looks at how well Indian law deals with the issue. The main point is that India is not short of legal provisions relating to online child safety. The problem is that there is a total lack of coordination between the various provisions. Child protection, criminal law, cyber law, evidence law and data protection have all developed in isolation, each governed by a different body. The result is that the level of protection afforded to the child is inconsistent and the treatment of a child in conflict with the law is highly unpredictable. The article looks at the issues of grooming and exploitation, offending by children and electronic evidence in child cases.

The approach is a doctrinal one, based on statutes, Supreme Court judgments and international standards. The guiding principle is that under the Juvenile Justice (Care and Protection of Children) Act, 2015 (JJ Act) and the Convention on the Rights of the Child (CRC), every decision must be made in the child's best interests and with a view to rehabilitation [3], [4], [5]. Part II is the legal framework, Part III is online grooming, Part IV is children in conflict with the law and Part V is electronic evidence. Parts VI to VIII are on rehabilitation, the proposed reforms and the conclusion.

II. THE LEGAL FRAMEWORK: A FRAGMENTED MAP

A. Child Protection and Juvenile Justice

The JJ Act is the foundation of the system [3]. Anyone under 18 is a child and a child in conflict with the law is one who has been accused or found guilty of an offence committed prior to the age of 18. The Act is built on the principle of innocence until proved otherwise, the principle of respect for dignity and privacy, the principle of confinement only as a last resort and the principle of a genuine opportunity to start again. The Protection of Children from Sexual Offences (POCSO) Act, 2012 sits alongside it and uses the same age threshold [6]. Its reach online is far

greater than one might initially think. Section 11 deals with persistent electronic communication with a child, threats to use real or fictitious images of a child's body or of a child in a sexual act and attempts to entice a child to engage in pornographic activity. Sections 13 to 15 cover the use of a child in pornography and the possession of such material. Sections 19 to 21 impose a duty to report and make failure to report an offence.

B. Cyber and Criminal Law

The Information Technology (IT) Act, 2000 covers the majority of online offences. Section 67B deals with the publishing or transmission of obscene material containing children (i.e. the publication or transmission of any sexually explicit depiction of a child), the collection, browsing, downloading or distribution of such material and the use of a child in an online relationship for the purpose of committing a sexually explicit act [7]. Sections 66C, 66D and 66E (relating to identity theft, personation and privacy violations) are also relevant to sextortion and the misuse of images [7]. Offences committed on or after 1st July 2024 will be prosecuted under the Bharatiya Nyaya Sanhita, 2023 (BNS) and the relevant provisions of the BNS on sexual harassment, voyeurism, stalking, extortion and criminal intimidation will apply [8]. The procedure will be governed by the Bharatiya Nagarik Suraksha Sanhita, 2023 [9] and the proof of electronic records will be governed by the Bharatiya Sakshya Adhiniyam, 2023 (BSA) [10].

C. Platforms and Data Protection

Platform liability is primarily governed by section 79 of the IT Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [11]. In *Shreya Singhal v. Union of India* section 79(3)(b) was read down so that the safe harbour is only lost where there is actual knowledge of the illegal content, that knowledge being obtained via a court order or government notification [12]. The 2021 Rules require intermediaries to warn users against the hosting of content which is paedophilic in nature or otherwise damaging and require larger social media intermediaries to make reasonable efforts to detect child sexual abuse material through the use of technology. The February 2026 amendments extend these provisions to synthetically generated information which is relevant to the morphed and artificial images discussed in Part IV [13].

The Digital Personal Data Protection Act 2023 (DPDP Act) introduces a data layer [14]. Section 9 of the Act requires a data fiduciary to obtain verifiable parental consent prior to processing a child's personal data, to refrain from processing which would be likely to harm the child's well-being and from tracking the child's behaviour or targeting the child with advertising. The Digital Personal Data Protection Rules 2025 (notified 13th November 2025) set out in Rule 10 how such parental consent is to be verified [15]. These obligations have not yet commenced. The DPDPA provisions came into effect on notification but s.9 and Rule 10 will only come into force 18 months later, in May 2027. For the moment the data protection law establishes a future obligation and provides no actual protection for children.

Each of those instruments is internally coherent. Taken together they are not. POCSO is dealt with via special courts, the IT Act via cyber cells, the JJ Act via the Juvenile Justice Boards (Boards) and the Child Welfare Committees (CWCs) and data protection via the Data Protection Board. There is no single body that owns the issue. All four of the Acts treat a person under 18 as a child, but the consequences of that are very different in each case and there is no Act that says what happens when a child is caught in two of them. You have the situation where a child is both a victim and an accused (a situation which is far more common than is generally recognised) and you have to go through multiple systems which don't interface at all.

III. ONLINE GROOMING AND CHILD VICTIMS

Grooming is the process whereby an offender slowly builds a relationship of trust with a child, typically by presenting himself as a friend or a romantic interest in order to abuse or exploit the child. There is no definition of grooming in Indian law and no offence of grooming per se. Prosecutors therefore have to rely on adjacent provisions: section 11 of POCSO which covers repeated electronic contact and enticement and section 67B(c) of the IT Act which covers the cultivation, enticement or inducement of a child into an online relationship for the purpose of sexually explicit conduct. POCSO also covers attempts and abetment.

This approach has a fatal flaw in that grooming is a process rather than a series of discrete acts and weeks of manipulative conversation which have left the child in a confused and isolated state may not amount to any offence at all. Other systems act earlier. In England and Wales both meeting a child as a result of sexual grooming and sexual communication with a child are criminal offences [16], [17]. The Lanzarote Convention has a similar provision and asks its parties to criminalise the use of information technology to solicit a child for sexual purposes [18]. The

Convention offence is one of proposing to meet and then going on to commit material acts and India is not a party to the Convention, but it is still a useful drafting point.

The Supreme Court (SC) in *Just Rights for Children Alliance v. S. Harish* reinforced the protection of the child victim [19]. The Madras High Court (HC) had set aside the case against a man who was accused of having such material on his phone, holding that mere possession without any intention to share it was not an offence. The SC disagreed with that approach. It held that s.15 of POCSO creates three distinct offences, that possession can be constructive and that the mere act of possessing such material without deleting it or reporting it can be a sufficient basis for an inference of intention to transmit. The Court also recommended that Parliament consider substituting 'child pornography' with 'child sexual exploitative and abuse material' (CSEAM), that the Union consider doing so by ordinance in the interim and that the courts should not use the older term in any orders or judgments. A recommendation is not an amendment. As far as we can verify for the purposes of this article the statute itself remains unchanged so the new term is a binding direction on the courts as to usage and does not in any way alter the offence. The article will use the Court's term for the material [20], with the caveat that POCSO itself still refers to child pornography.

Two further points from the judgment are of some significance. The Court regarded the dissemination of the material as an ongoing harm to the child in the image, rather than merely as an issue of obscenity. It also recommended that there should be comprehensive sex education and early intervention for children who are displaying problematic sexual behaviour. Many of these children will be minors themselves and will be likely to come before a Juvenile Justice Board. The recommendation thus brings the protective and juvenile justice elements of the system into conjunction (the two are otherwise kept distinct by the statutes). It also raises a question which the case itself did not address. Where a child has the image of a peer and keeps or passes it on, s 15 may apply in its own terms and the appropriate response will be one dictated by the JJ Act rather than by the adult prosecutions at issue.

IV. CHILDREN IN CONFLICT WITH LAW ONLINE

The tricky ones are when the child is the one being accused. A teenager might share a very intimate image of a classmate, create a morphed or fake image, run an account to harass another student or get involved in a sextortion scheme. Some of those actions are clearly malicious. Many are just poor judgement and a total lack of awareness as to how permanent online material is. The JJ Act requires the system to be able to draw the line between the two, but that line is often very blurred. You have two teenagers in a relationship sharing images with each other and both of them are children. POCSO contains no specific carve out for consensual image sharing between two children. The line has to be drawn by the discretion of the police, the prosecutors and the Boards and that is an extremely shaky basis on which to make such a significant decision.

Three features of the JJ Act are relevant here. It classifies offences as petty, serious and heinous depending on the punishment prescribed and an offence is only heinous if the minimum punishment is 7 years or more of imprisonment [3]. *Shilpa Mittal v. State (NCT of Delhi)* dealt with the gap in the categories [21]. Where the maximum is over 7 years but there is no minimum or the minimum is less than 7 years the offence is not heinous and the Court held it to be a serious offence until Parliament stepped in. The 2021 amendment subsequently codified that position in s.2(54) [22]. For online offending this has a significant impact. Section 67B of the IT Act and the BNS provisions which are the ones most commonly encountered online do not have a minimum punishment of 7 years and so are either petty or serious offences and trial as an adult does not follow. The situation only changes where a child is alleged to have committed an offence which has a high minimum (e.g. penetrative sexual assault under POCSO which can arise in grooming cases involving older adolescents). *Shilpa Mittal* therefore keeps the vast majority of digital offences within the Board's remit for rehabilitation as heinousness is a matter of the statutory minimum and not of the perceived gravity of the harm.

Secondly, where a child aged between 16 and 18 is charged with a heinous offence the Board must make a preliminary assessment of the child's mental and physical capacity, their ability to appreciate the consequences and the circumstances of the offence. Capacity in this context has a digital dimension. A child may well have understood the act itself but not have appreciated how far and how permanently an image can travel. The statutory criteria do not make that distinction. The Board will need expert assistance

to answer that question and the availability of such assistance is a matter for empirical study.

Thirdly the Act provides for rehabilitative orders (advice or admonition, group counselling, community service, a fine where appropriate and release on probation). These are very well suited to the online offences. A child who has shared a classmate's image for example needs to understand the concept of consent and the harm that has been done to the other child. Detention doesn't really teach that and counselling and community service can.

The Act also protects the child throughout the process. Where a child is apprehended by the police they must be placed with a special juvenile police unit or a designated child welfare police officer and produced before the Board within 24 hours (the Act is clearly in favour of release on bail). Section 74 prohibits the disclosure of the child's identity. That's important as screenshots, videos and names can go viral on social media long before any hearing takes place.

Age is also a threshold issue. Section 94 mandates that the Board shall determine age from school records, a birth certificate and if neither of those is available then from a medical examination [3]. In *Pratap Singh v. State of Jharkhand* a Constitution Bench held that it is the date of the offence which determines whether a person is a juvenile [23]. Online conduct of course is a bit more complicated in that the act of holding or sharing material may go on long after the individual has turned 18 and it is not immediately obvious which of those acts is the relevant one. The Supreme Court has accepted 18 as a legitimate policy position and that position has been upheld in both *Salil Bali v. Union of India* and *Subramanian Swamy v. Raju* [24], [25], [26]. The real issue is how well the system works for the children it already covers.

V. DIGITAL EVIDENCE AND THE CHILD

Electronic evidence is at the heart of almost every online case and it is in that area that the interests of the investigator, the victim and the accused child come into conflict. Section 63 of the BSA now deals with admissibility (replacing section 65B of the Indian Evidence Act, 1872). The old law in *Anvar P.V. v. P.K. Basheer* treated the section 65B(4) certificate as a pre-requisite for secondary electronic evidence and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* affirmed that position though went on to say that the certificate would not be required where the device itself is produced in court [27], [28]. Section 63 continues to require the certificate, requires a hash and requires the signature of both the person in charge of the device and an expert [10].

These rules were designed for adult litigants and in the context of children give rise to three issues. The first is the issue of secondary harm. The material that is seized may itself be CSEAM material of a child victim and each copy, each printout, each viewing will in effect re-injure the child. The rules should therefore limit copying, identify files by hash rather than by the file itself, and restrict access. Since possession is the essence of the section 15 offences, it is important to make it absolutely clear that lawful custody for the purpose of investigation is not the same as possession of the kind which the offence is concerned with. The second issue is the device of a child accused. A seized phone contains the whole of a young person's life so seizure must be proportionate and data which is not relevant to the case in question must not be touched. The third is capacity. Where police units and Boards do not have access to forensic support, certificates are delayed or defective and a case can fall apart or a child can end up in the system for longer than is necessary.

POCSO does have child-friendly procedures in place (recording the child's statement at a place of their choice, use of audio/video etc). The POCSO and JJ Act say very little about what happens to the digital material once it's on the file though. The DPDP Act doesn't really close the gap either as it has an exemption for the processing of personal data for the purpose of investigating an offence. That means that the police in custody are still required to respect the child's device privacy via procedure. Guidelines can provide that procedure without the need for new legislation.

VI. REHABILITATIVE JUSTICE IN A DIGITAL SETTING

Rehabilitation is the thread that runs through the JJ Act. The SC recognised this right at the outset in *Sheela Barse v. Union of India* where it was critical of the incarceration of children and called for a separate Juvenile Justice system [29], [30]. The problem now is that the rehabilitative orders under the Act are very broad and don't deal with digital behaviour or image based abuse at all. A child who has groomed another is in need of a very different form of rehabilitation to a child who has been groomed and a child who has done both may in fact need both.

Rehabilitation must also extend to the victims themselves who will require counselling, removal of the material and assistance in restoring trust. Removal

is difficult given the speed at which content spreads and the ease with which it reappears. The platform's obligations and data protection law are both of assistance, but the article makes no reference to any provision that links the two to the child protection system. Takedown under the intermediary rules is achieved via a notice to the platform and there is nothing in the process which connects it to the Child Welfare Committee which may be in the process of supporting the child.

VII. THE WAY FORWARD

Reform doesn't need a new code. It just needs better links between the laws we already have. Five measures in particular seem the most useful (each of them is a proposal, not an existing obligation).

Firstly the Government should have a National Protocol for online child safety cases which clearly defines who does what and brings together the Police, the Cyber Cells, the Boards, the CWCs and the Special Courts with the Ministries of Women and Child Development, Home Affairs and Electronics and Information Technology, with shared ownership.

Secondly Parliament should define online grooming in POCSO and follow the Supreme Court's suggestion on the terminology. The offence would be one of an adult grooming a child (could be based on an age gap or abuse of trust) and would not cover ordinary conversation between adolescents.

Thirdly Boards and prosecutors will need guidance in relation to children who commit offences online (in particular those who share the images of their peers). A graduated approach, starting with counselling and computer literacy and reserving formal proceedings for the most serious of cases is the right approach in the context of the JJ Act. The guidance should also cover the application of POCSO where both parties are minors.

Fourthly a digital evidence protocol for cases involving children should permit limited copying, hash based identification, restricted access and proportionate searches of the children's devices with the appropriate trained forensic examiner to ensure that the section 63 certificates are both accurate and timely.

Fifthly, the organisations dealing with these cases need to be trained and resourced. In *Sampurna Behrua v. Union of India* the Supreme Court looked at the implementation of the JJ Act and directed that the Boards, the CWCs and the juvenile police units be strengthened [31]. The same applies to digital skills. When section 9 of the DPDP Act and Rule 10 come into force in 2027, data protection can be used to make children's services safer by design but only if the Data Protection Board and the child protection authorities work together.

VIII. CONCLUSION

The promise of juvenile justice hasn't changed in the information age. A child who has committed an offence should be understood and helped and a child who has been harmed should be protected and heard. What has changed is the context. India has a number of well-intentioned laws in place to protect children online but they operate in silos. Some of the most important ones (such as the parental consent provisions under the data protection law) have yet to come into force. The real challenge is coordination. We need to have a clear understanding of what constitutes an offence, we need to be able to properly administer electronic evidence, we need to have the right institutions in place and we need rehabilitation that is relevant to the child's online world. The real test is whether the system can protect the child on one side of the screen and reform the child on the other, with an awareness that in many cases they are the same child.

REFERENCES

[1] UNICEF, *The State of the World's Children 2017: Children in a Digital World* (2017).

[2] Sonia Livingstone, John Carr & Jasmina Byrne, *One in Three: Internet Governance and Children's Rights* (Global Comm'n on Internet Governance, Paper Series No. 22, 2015).

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

[4] Convention on the Rights of the Child, 20th November 1989, 1577 U.N.T.S. 3.

[5] U.N. Comm. on the Rts. of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (2 Mar. 2021).

[6] Protection of Children from Sexual Offences Act, 2012, No. 32 of 2012, India Code (2012).

[7] Information Technology Act, 2000, No. 21 of 2000, India Code (2000).

[8] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, India Code (2023).

[9] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, India Code (2023).

[10] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, India Code (2023).

[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E).
[12] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[13] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (notified 10th February 2026).
[14] Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).
[15] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025).
[16] Sexual Offences Act 2003, c. 42 (UK).
[17] Serious Crime Act 2015, c. 9 (UK).
[18] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 25 October 2007, C.E.T.S. No. 201.
[19] *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716.
[20] ECPAT Int'l, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (2016).
[21] *Shilpa Mittal v. State (NCT of Delhi)*, (2020) 2 SCC 787.
[22] Juvenile Justice (Care and Protection of Children) Amendment Act, 2021, No. 23 of 2021, India Code (2021).
[23] *Pratap Singh v. State of Jharkhand*, (2005) 3 SCC 551.
[24] *Salil Bali v. Union of India*, (2013) 7 SCC 705.
[25] *Subramanian Swamy v. Raju*, (2014) 8 SCC 390.
[26] Justice J.S. Verma Comm., *Report of the Committee on Amendments to Criminal Law* (Jan. 23, 2013).
[27] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[28] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[29] *Sheela Barse v. Union of India*, (1986) 3 SCC 632.
[30] Ved Kumari, *The Juvenile Justice System in India: From Welfare to Rights* (Oxford Univ. Press 2004).
[31] *Sampurna Behrua v. Union of India*, (2018) 4 SCC 433.